

COLLECTIVE EXHIBIT 1

The Internet of Money

A COLLECTION OF TALKS BY
Andreas M. Antonopoulos
VOLUME ONE

Foreword by Don Tapscott

The Internet of Money

Praise for "The Internet of Money"

I've always wondered what would have happened if we had built one-click payments into the browser from the very beginning. With bitcoin, we finally get this Internet of Money. But this book isn't just an ode to bitcoin — it's an ode to open protocols, what happens when you connect people online, and the power of innovation on the internet.

— Marc Andreessen, co-founder Netscape and Andreessen Horowitz

With Mastering Bitcoin, Andreas M. Antonopoulos wrote one of the best technical books on digital currency. With The Internet of Money, he's matched that feat by compiling his talks into one of the best books on Bitcoin for a broad audience. Highly recommended!

— Balaji Srinivasan, CEO 21.co

Over the past three years, awareness of the sweeping, transformative potential of bitcoin and its underlying blockchain technology has grown exponentially. That required people to grasp not only how this unorthodox technology worked but also its profound promise for society. No one has done more than Andreas Antonopoulos to get them over that hurdle. Read him. It will make you wiser.

— Michael J. Casey, co-author The Age of Cryptocurrency: How Bitcoin and Digital Money are Challenging the Global Economic Order

Foreword

By Don Tapscott

In early 2014, my son Alex and I began the research for our book *Blockchain Revolution*. I had been working on the 20th anniversary edition of *The Digital Economy* and reflecting on the last two decades and what's next, I had become fascinated by Bitcoin and cryptocurrencies. Meanwhile, Alex was an executive with the investment bank Canaccord Genuity. He noticed the growing enthusiasm of early stage bitcoin and blockchain companies in 2013 and began leading his firm's efforts in the space. During a father-son ski trip to Mt. Tremblant in early 2014, we brainstormed over dinner about collaborating on this topic and to make a long story short decided to write a book.

We were aware of the writings of Andreas M. Antonopoulos, and our work quickly drew us into the extensive collection of his speeches on YouTube. I remember watching and re-watching them for hours and taking extensive notes throughout. Both Alex and I were struck with the depth of his knowledge, his fluency explaining complex concepts, and his clarity of thinking. Here was someone who presents the most difficult of topics in simple terms using strong analogies and with passion and insight in every talk. I remember thinking "how can this guy know so much about something so new?"

In **one video in 2013** he was filmed talking to others around a table – but YouTube revealed that tens of thousands of people had watched the discussion. In another he showed great alacrity in the face of adversity, most memorably in a brilliant talk about **"Bitcoin Neutrality"** to a large convention hall with only two people seated in it. When the camera zoomed in you might think he was talking to a full theatre based on his energy and expressiveness.

It was good he persevered. Fortunately, both these and other talks were captured by video and we can all benefit today. With the publication of *The Internet of Money*, tightly edited versions of these lectures are sure to be received thankfully by many, including me. The talks are each unique (no canned presentations here), unscripted and compelling. There are few people who have the abilities to speak extemporaneously on any tough topic, let alone on this one.

The early days of most technological revolutions are dominated by the builders, and there is typically a dearth of deep conceptualizing and lucid explanation. After all, it took decades after the creation of the Arpanet — the early incarnation of the internet — for big thinkers to dig into the implications of what

the first generation of the digital revolution might mean for our lives. So it was with the second era of the Internet — the technology behind digital currencies. The first years of Bitcoin were dominated by developers and then speculators — both practitioners, in a sense. Early advocates presented theories about how this new technology could free us from the shackles of government but the world needed more than ideological missives to understand the importance broader significance of crypto currencies. We also needed someone to explain how all this stuff worked.

Put simply, Andreas stepped up. In fact, I'll bet history will remember that there was no one who played a more important role in the early days of explaining Bitcoin, what it is and what it means. Needless to say when it came to doing in-depth interviews of thought leaders for our own book, we pretty much started with Andreas.

Reading this collection of essays, it's amazing to contemplate that Andreas was waxing poetic and profound years before hardly anyone had even heard of Bitcoin. However don't read this for the historical record of a furtive mind. Rather, read it for its rich insights, which are equally relevant, if not more relevant, today.

Andreas was on to something big, early. Alex and I agree that a new kind of Internet is in the making. For the last decades we've had the Internet of Information, but today we're witnessing the birth of the Internet of Value or as Andreas calls it The Internet of Money. Everyone, dear reader, needs to understand this revolution as its impact will surely be as great or greater than the first era.

Parenthetically, let me note that as a Canadian I'm a direct beneficiary of Andreas' furtive mind. In March 2014, the Canadian Senate authorized the Standing Senate Committee on Banking, Trade and Commerce to study digital currencies, with a particular focus on their potential risks, threats and advantages. The Senate's initial interest in the topic was negative, somewhat motivated by media reports about Bitcoin being used to launder money and commit crime. Andreas **testified** before the committee and his session is now somewhat legendary in blockchain lore. As one Senator told me "he blew our minds" (a tough thing to do for the gentlemen of this austere Canadian "Chamber of sober second thought").

When all was said and done the Senate issued a stellar report that emphasized the positive opportunities and took a strong position against pre-mature regulation and interference in the blockchain revolution. Thank you Andreas.

Enjoy this book. If you're new to the topic, prepare to join Canada's sober Senators and have your mind blown too. If you think you know all there is to know, prepare to be humbled and inspired. I am thankful Andreas took the time to capture these videos in text as this tome will make an important contribution to our mutual challenges of ensuring that this new Internet fulfills its enormous potential.

Don Tapscott, Lake of Bays, Ontario Canada. August 20, 2016.

*Don Tapscott is the author of 15 books on new technology in society, including **Paradigm Shift, Growing Up Digital, The Digital Economy, Wikinomics,** and most recently with his son Alex **Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money Business and the World.** He is the CEO of the think tank The Tapscott Group; an adjunct Professor at the Rotman School of Management, University of Toronto and an Associate of the Berkman Klein Center for Internet and Society at Harvard University.*

Preface

By Andreas M. Antonopoulos

When I started my journey in bitcoin, I never thought it would lead to this. This book is like an abridged diary of my discovery of bitcoin, delivered through a series of talks, starting in 2013 continuing to early 2016.

Over these past three years, I have delivered more than 150 talks to audiences across the world, recorded more than 200 podcast episodes, answered several hundred questions, participated in more than 150 interviews for radio, print and TV, appeared in eight documentaries and written a technical book called *Mastering Bitcoin*. Almost all of this work is available, for free, under open-source licenses, online. The talks included in this book are only a small sample of my work, selected by the editorial team to provide a glimpse into bitcoin, its uses, and its impact on the future.

Each of these talks was delivered to a live audience, without slides or any visual aides, and was mostly improvised. While I have a topic in mind before each talk, a lot of my inspiration comes from the energy and interaction with each audience. From talk to talk, the topics evolve as I try out new ideas, see the reaction and develop them further. Eventually, some ideas that start as a single sentence evolve, over several talks, into an entire topic.

This process of discovery is not perfect, of course. My talks are littered with minor factual errors. I recite dates, events, numbers, and technical details from memory and often get them wrong. In this book, my off-the-cuff errors, malapropisms, and verbal ticks have been cleaned up by the editors. What remains is the essence of each presentation — how I wish it had been delivered, rather than a transcript of the actual delivery. But, with that cleanup there is also a price to pay. What is missing is the reaction and energy of the audience, the tone of my sentences, the spontaneous giggles from me and the people in the room. For all of that you have to watch the videos which are linked in [*Appendix A, Video Links*](#) of the book.

This book and my work over the past three years is about more than bitcoin. They reflect my worldview, my political ideas and my hopes, as well as my technical fascination and my unabashed geekiness. They summarize my enthusiasm about this technology and the astonishing future that I envision. This vision starts with bitcoin, a quirky cypherpunk experiment which unleashes a ripple of innovation, creating "The Internet of Money" and radically

transforming society.

Note from the Editors

Almost the entire bitcoin community knows Andreas's contribution to bitcoin. In addition to his written and audio work, he's a highly sought-after public speaker, lauded for consistently delivering innovative, thought-provoking, engaging talks. This book represents only a small sampling of Andreas's work in the bitcoin and blockchain industry over the past three years. With so much content, simply deciding what talks to include was an arduous task. We selected these specific talks because they fit the criteria of the book; we could easily have included dozens more. This book is Volume 1; we hope to publish another volume soon.

We began this book project with a vision: to provide an easy-to-read, short-story style overview of why bitcoin matters, of why so many of us are excited about it. We wanted something we could share with family, friends, and co-workers that they might actually read: a compendium that they could pick up for five minutes, no-commitment, or explore for a few hours. It needed to be engaging, with real-world analogies to make the tech understandable. It needed to be inspirational, with a vision of how these things could positively impact humanity. It needed to be honest, acknowledging the shortcomings of our current systems and the technology itself.

Despite our best efforts, we're sure there are things we could improve and change; this is a first edition. We've edited heavily in some places, for readability, while always trying to preserve the essence of the talk. We believe we've struck a good balance and we're pleased with the book as a whole. We hope you are too.

You may have noticed this work is copyrighted by Merkle Bloom LLC. Andreas has granted us a license to modify and distribute the work in this way. If you would like to use portions of our book in your project please send a request to copyright@merklebloom.com. We believe in open-source and information freedom; we grant most license requests quickly and free of charge.

Tips to make your reading experience even better: Each talk is intended to stand alone. There is no need to start at the beginning — although if you are unfamiliar with bitcoin, you may want to start at the first talk, "What is Bitcoin," to get an overview of the topic. You'll notice some repeating themes and analogies, like the Red Flag Act or the parent-and-child talk about money. While the examples occasionally repeat, they're most often used to illustrate a different point in each talk.

You'll find a robust index at the end of the book. One of the things we're most proud of is the index. We've worked hard to provide an index that will allow you to cross-reference and research themes and topics.

Chapter 1. What Is Bitcoin?

Disrupt, Start-up, Scale-up; Athens, Greece; November 2013

Video Link: <https://www.youtube.com/watch?v=LA9A1RyXv9s>

Reader note: This talk was given in late 2013. Bitcoin transactions are no longer free but fees are minimal. Currently, transaction fees are approximately 10 cents per transaction, regardless of the monetary value of the transaction.

Good afternoon, Athens! Thank you for having me today. You want *disrupt*? I've got disrupt. I've got downright revolution. Today, we're going to talk about the most exciting, most interesting, and probably the most important technological invention in computer science of the last 20 years. I'm here to talk about bitcoin.

Bitcoin is digital money, but it's so much more than that. Saying bitcoin is digital money is like saying the internet is a fancy telephone. It's like saying that the internet is all about email. Money is just the first application. Bitcoin is a technology, it is a currency, and it is an international network of payments and exchange that is completely decentralized. It doesn't rely on banks. It doesn't rely on governments.

"Saying bitcoin is digital money is like saying the internet is a fancy telephone."

We have never done this before in the history of humanity. This invention is truly revolutionary. When we look back, we will see that this is a historic moment in the evolution of computer science, but it is also a social and political revolution in the making. So, let's get started.

1.1. Bitcoin, the Invention

Bitcoin is digital money. It is money just like euros or dollars, only it's not owned by a government. You can send it from any point in the world to any other point in the world instantaneously, securely, and for minimal or no fees at all. Two days ago, we saw one of the largest transactions ever recorded on the bitcoin network, where someone transferred \$150 million between two bitcoin accounts, in one second, for zero fees. Just that allows you to grasp how disruptive this technology is going to be in terms of international payment systems. But this is just the beginning.

Bitcoin is a digital currency that came into existence in 2008 as an invention by a person called Satoshi Nakamoto. He published a paper where he posited that he had found the way to create a decentralized network that could achieve consensus, agreement, without any central controlling authority. Now, if you have studied computer science or distributed systems, this is known as the *Byzantine Generals' Problem*. It was first described in 1982. Until 2008, it was an unsolved problem. Then, Satoshi Nakamoto said, "I have solved it." Guess what happened next? Everybody laughed, ignored him, and dismissed him. He published his paper, and three months later, he published software that allowed people to start building the bitcoin network.

Bitcoin is not a company. It is not an organization. It is a standard or a protocol just like TCP/IP, or the internet. It's not owned by anyone. It operates by simple mathematical rules that everyone who participates in the network agrees on. Through this simple mechanism, through this invention of Satoshi Nakamoto, bitcoin is able to allow a completely decentralized network of computers to agree on what transactions have occurred on a network, essentially agreeing on who currently has the money.

So, if I send money from my account to somebody else's account in this peer-to-peer, completely decentralized network, it's just like sending an email. There's no one in the middle. Every ten minutes, the entire network agrees on what transactions have happened, without any centralized authority, by a simple election that occurs electronically.

This particular solution, this invention, is far more important than currency. Currency is just the first app—just the first application that you can build on a distributed consensus system. Other applications include distributed fair voting, stock ownership, asset registration, notarization, and many other applications we've never thought of before.

"This particular solution, this invention, is far more important than currency. Currency is just the first app."

I discovered bitcoin for the first time in 2011, and since the internet, I have not felt so completely overwhelmed by the possibilities that I saw. I was there at the dawn of the internet in 1991 when it was pre-commercial. I could see that this was going to change the world but no one believed me. I have that exact same feeling about bitcoin.

Now, some of you may have heard of bitcoin, as a currency, is wildly high in price one day and wildly low in price the next. I'm here to tell you to ignore the price, to ignore bitcoin the money, and understand bitcoin the technology, the invention, and the network it creates. If we mess up the money, we'll just reboot another currency. The invention of bitcoin, the technology that makes it possible, cannot be uninvented. It creates the possibilities for decentralized organization on a scale never before seen on this planet.

"The invention of bitcoin, the technology that makes it possible, cannot be uninvented. It creates the possibilities for decentralized organization on a scale never before seen on this planet."

1.2. Money of the People

Here's why bitcoin is important to me.

Approximately 1 billion people currently have access to banking, credit, and international finance capabilities—primarily the upper classes, the Western nations. Six and a half billion people on this planet have no connection to the world of money. They operate in cash-based societies with very little access to international resources. They don't need banks. Two billion of these people are already on the internet. With a simple application download, they can immediately become participants in an international economy, using an international currency that can be transmitted anywhere with no fees and no government controls. They can connect to a world of international finance that is completely peer-to-peer. Bitcoin is the money of the people. At its center are simple mathematical rules that everyone agrees on and no one controls. The possibility of connecting these 6 1/2 billion people to the rest of the world is truly revolutionary.

"Bitcoin is the money of the people."

Payment processors are going to be affected. These enormous companies charge higher fees to send money to poorer destination countries, a situation that is exploitative and corrupt. These organizations make enormous profits for a function that can be done in bitcoin nearly for free. As the adage of the entire internet once went, "I just replaced your entire industry with 100 lines of Python code," that's exactly what we're doing with bitcoin.

1.3. Currencies, Businesses, and International Payments

How can you use bitcoin today? Simply speaking, bitcoin can operate as a currency. You can think of it as buying a foreign currency: You can connect to an exchange over the web, wire some euros, and use those euros to buy bitcoins at the current exchange rate. Yet, that's not really the best way to do it. We're entrepreneurs, right? We want to disrupt. The best way to do it is to find a product or service that you can offer that someone with bitcoin wants to buy, and start *earning* bitcoin.

1.3.1. Solving Payment Problems

If you think about starting up a business in an international environment, there are two primary barriers to becoming a global business. The first barrier is that it is difficult to transport products and services across borders. With the internet, we solved that. We can now create products and services that are virtual, ones that we can sell anywhere in the world. So, we can deliver the product, but we still have one big problem: How do we get paid? Bitcoin solves that part. It allows us to receive payments from anywhere in the world, instantaneously. The bitcoin network allows any individual to send an amount that is as small as 100-millionth of a bitcoin, which in today's terms is a very tiny amount of money. You can't do that with today's money and payment systems. Credit cards were made in the 1950s, and they were most certainly not made for an internet age. Bitcoin is made for the internet age.

"Credit cards were made in the 1950s, and they were most certainly not made for an internet age. Bitcoin is made for the internet age."

So, if you can suddenly send payments that are one-hundredth of a euro, or one-thousandth of a euro, you can sell content. You can do microtransactions. You can collect payments from millions of people in tiny amounts and make them, in aggregate, be worth something. On the same network where you can send one-thousandth of a euro or one-millionth of a euro, you can send a billion euros or a trillion euros. The fee will be exactly the same, because fees depend on the size of the transaction in kilobytes, not on the amount or content.

1.4. Neutrality, Criminals, and Bitcoin

Let's look back at the internet and see what lessons we can learn about why bitcoin is important. One of the most important principles of the internet is neutrality. The internet does not distinguish between a large organization and a small organization. It does not know the difference between CNN and an Egyptian blogger. It allows the Egyptian blogger to speak to the world with the same power of voice that CNN has.

Bitcoin is neutral to the sender, the recipient, and the value of the transaction. That means it gives every citizen, every user of bitcoin, the ability to innovate in terms of financial instruments, payment systems, and banking. You can operate on the same level as Citibank. That is truly revolutionary.

"Bitcoin is neutral to the sender, the recipient, and the value of the transaction. That means it gives every citizen, every user of bitcoin, the ability to innovate in terms of financial instruments, payment systems, and banking."

It takes a hierarchical system of international finance and turns it on its head. Up to now, that hierarchical system has achieved security by limiting access, because that is the main method of trust in our payment systems—you can't get in unless you're vetted. Bitcoin creates a completely flat and decentralized network where every node is equal, where the protocol is neutral to the transactions, and it pushes innovations to the edge of the network, allowing exactly the same phenomenon we saw on the internet: innovation without permission. You don't need to ask anyone if your application can be published on the internet. You don't need to ask anyone to completely subvert a new industry with your information technology. On bitcoin, you don't need to ask anyone to invent a new financial instrument, a new payment system, a new service. You can just do it. You can just write the code, and you are now part of an international financial network that can run that code and put you in contact with millions of consumers.

"On bitcoin, you don't need to ask anyone to invent a new financial instrument, a new payment system, a new service. You can just do it."

Now, it's still early days. We don't yet have the polished interfaces. It's difficult to use. It's used by criminals. It's used by various organizations around the world, and it's not easy to see exactly who is using bitcoin. I've heard all of that before. When I was on the internet back in 1991, it was a den of thieves, pornographers, pirates, and criminals. But it didn't matter then, and it doesn't matter now. It doesn't matter because the same powerful technology that can be

used by a criminal to promote their criminal activities can also be used by all of the rest of us to do good, to do incredible things all across the world. And there are more of us than there are of them.

Bitcoin creates an environment that is ripe for innovation, because it's not just a currency; it's a technology, a network, *and* a currency. I can tell you today that I'm very happy that bitcoin's price is climbing very high, because I own some bitcoin and it feels kind of nice. But I don't care about the price. If bitcoin crashed tomorrow morning, the technology is still revolutionary. Just like if a website fails on the internet, or an application fails on the internet, the internet doesn't go away.

"Bitcoin creates an environment that is ripe for innovation, because it's not just a currency; it's a technology, a network, and a currency."

1.5. Bitcoin as a Mechanism to Opt In and Opt Out

If you understand that bitcoin is a technology and not just a currency, you can truly grasp the importance it has. Again, it's not about us. It is about the other 6 1/2 billion. It is about the ability to bring to the world a level of financial integration that the world has never seen before. From our perspective in the privileged world, it is a great technology. We can do some disruptive innovation. We can build some interesting services. But if you're a Kenyan farmer who's trying to raise money in order to buy seed, and now you can do decentralized peer-to-peer lending and reach out to lenders from all across the globe, this is not just a technology—this is truly life-changing.

"Bitcoin is about the ability to bring to the world a level of financial integration that the world has never seen before."

The vast majority of the world lives under repressive and corrupt regimes with central banks that impose hyper-inflation at 30 percent a month. It's much more important to see how bitcoin can affect all of those people. There are 2 billion people on the internet and only 1 billion of them have bank accounts. We can change that. It's not going to be easy, make no mistake about it. When you throw a disruptive technology in the middle of the most powerful organizations on the planet, they don't like it. Right now, we're still in the early stages. To use the trite expression, "First they ignore us, then they laugh at us, then they fight us, then we win." We're still at the laughing-at-us stage. That's quite all right, because by the time they get to fighting us, they've already lost. This technology just went global with the introduction of more than \$2.5 billion from Chinese investors who discovered a counterbalance to the world domination of the global reserve currency of the US dollar.

1.5.1. Altcoins: Currencies for Everyone

There are almost 200 currencies of the world, but there's only one international currency. There are almost 200 currencies controlled by central banks and governments, but there is only one mathematical currency today, and that is bitcoin.

"Cryptographic currencies are going to be a mainstay of our financial future. You cannot un-invent this technology. You cannot turn this omelette back into eggs."

We are going to build more of them. Cryptographic currencies are going to be a mainstay of our financial future. They are going to be a part of the future of this planet because they have been invented. It's as simple as that. You cannot un-invent this technology. You cannot turn this omelette back into eggs. We already have over 100 competing currencies in the space, which shows how quickly innovation has exploded, even beyond bitcoin the currency. There are many other alternative currencies — altcoins, as they're known—that use the same basic technology of a decentralized asset ledger using consensus in the network with Satoshi's algorithm. Some of these currencies are inflationary, some deflationary, some use demurrage or negative interest rates, some are charitable and redistribute a proportion of the income to charitable organizations.

We can invent money nonstop and create new forms of money and financial instruments.

"At the end of the day, bitcoin is programmable money. When you have programmable money, the possibilities are truly endless."

1.6. Programmable Money for All of Us

At the end of the day, bitcoin is programmable money. When you have programmable money, the possibilities are truly endless. We can take many of the basic concepts of the current system that depend on legal contracts, and we can convert these into algorithmic contracts, into mathematical transactions that can be enforced on the bitcoin network. As I've said, there is no third party, there is no counterparty. If I choose to send value from one part of the network to another, it is peer-to-peer with no one in between. If I invent a new form of money, I can deploy it to the entire world and invite others to come and join me.

"Bitcoin is the internet of money. Currency is only the first application. At its core, bitcoin is a revolutionary technology that will change the world forever."

Bitcoin is not just money for the internet. Yes, it's perfect money for the internet. It's instant, it's safe, it's free. Yes, it is money for the internet, but it's so much more. Bitcoin is the internet of money. Currency is only the first application. If you grasp that, you can look beyond the price, you can look beyond the volatility, you can look beyond the fad. At its core, bitcoin is a revolutionary technology that will change the world forever.

Join me in the revolution.

Thank you.

Chapter 2. Peer-to-Peer Money

Reinvent Money at Erasmus University; Rotterdam, Netherlands; September 2015

Video Link: <https://www.youtube.com/watch?v=n-EpKQ6xIJs>

A lot of people ask me to talk about the latest things in bitcoin, but what I really want to talk about is ancient history. I want to provide a historical context for money and talk about why bitcoin is important in this historical context.

2.1. How Old Is Money?

First, a little pop quiz for the audience: If you think of money as technology, as a technological system that human civilization has invented, how old is this technology? Any ideas? *Audience responds with wildly varying answers*

Lots of different answers here. It's always surprising to me that people say, it's 400 years old, 1000 years old, 2000 years old. In fact, we don't really know how old money is. Part of the reason we don't know how old money is, is because we have yet to discover a civilization so old that it didn't have money. We know money is as old as civilization.

"Money is as old as civilization."

One thing that surprises people is that money is older than writing. We know this because when we look at archeological discoveries of writing, we find hieroglyphics and we find cuneiform. When we look at all of these ancient forms of writing, guess what they're writing about? Money. They're writing ledgers. All of the ancient writing we find, the first forms of writing, are ledgers. They are writing about money. Because money is older than writing.

Is money older than the wheel? I don't know, but we do know that wheels were used as money. Perhaps the first wheel was sold for money or was used as a form of money itself. Archeological sites going back into the Stone Age have revealed the presence of money in the form of shells and feathers and beads.

In fact, we can teach primates how to use money. There have been several studies where chimpanzees are taught how to use money. They are taught that a specific type of stone can be exchanged for bananas. Researchers then watch the monkeys to see what they will do with this new information. They very quickly invent armed robbery. They figure out that if you beat up the other monkey and take its stones, you can exchange them for bananas. Surprisingly, the second thing they invent is prostitution. They figure out that sexual favors can be exchanged for stones, which can be used for bananas. What does that tell you about the nature of money?

I think the important insight into the nature of money is that money is a form of communication. At its very basic level, money isn't value. Money represents an abstraction of value; it's a way of communicating value. It's a language. Therefore, money is as old as language because the ability to communicate value is as old as language and money. In many ways, it has characteristics that make it a linguistic construct. It's a form of communication.

"We use money to communicate value to each other, to express to each other how much we value a product, a service, a gesture."

We use money to communicate value to each other, to express to each other how much we value a product, a service, a gesture. We use it as the basis of social interaction because by communicating value to each other, we create social bonds. So, money is also a very important social construct. This is an ancient technology. Yet, ironically, it's one of the technologies that is least studied from a historical and technology perspective. We look at bitcoin today and it represents an invention, a new form of money. Let's think about that for a moment.

2.2. Technological Evolution of Money

How often has the technology of money been transformed by invention? How many different forms of money have existed? At a very basic level, a way to communicate value is to exchange things that we consider of equal value. "Here is a goat. I will take 20 bananas for my goat." That's not really money because it's a barter transaction, but it's the first form of communication about value.

2.2.1. Barter to Precious Metals

Then, we start seeing abstract forms of money. The first major technological evolution is to start exchanging something that you can't eat—a feather, a bead, a string with knots on it, a colorful something that can be used for aesthetic purposes. That's when money takes an abstract form. The first major transformational technology moment for money was when money stopped being about the tangible consumption of intrinsic value, but became something that referred to value, as an abstraction.

"The first major transformational technology moment for money was when money stopped being about the tangible consumption of intrinsic value, but became something that referred to value, as an abstraction. One of the most popular forms of these abstractions was to use precious metals to express value."

One of the most popular forms of these abstractions was to use precious metals to express value. Precious metals combine some of the most important characteristics of money: hard to find (scarce); easily transportable (at least when compared to a giant rock or a whole barrel of feathers); easy to divide (you can cut a gold coin into pieces and subdivide the pieces); and universally valued for aesthetic purposes. That's the second major transformation in money technology. It took hundreds of thousands of years before we saw the introduction of precious metals. Historically, we start seeing precious metals in the beginning of the agrarian civilizations in the Fertile Crescent area in the Middle East. The Babylonians, the Egyptians, and the Greeks developed these precious metals.

2.2.2. Precious Metals to Paper

Two major technological evolutions and then nothing for a few thousand years. Then someone came up with a brilliant idea: If I deposit gold with someone trustworthy, they can give me a piece of paper that says that I have gold in this trustworthy vault. Then I could trade the paper instead of the gold. It's easier to carry. As long as I can trust that my money is in the vault, then I've got a new form of money.

With every technological evolution in money, there is skepticism. But I think this might be the moment of the greatest amount of skepticism in human civilization. For a lot of people, this new invention of money as paper was somewhat controversial. You think people are freaking out about bitcoin? Imagine how much they freaked out when you told them that now, instead of trading in gold, they would trade in pieces of paper. For a lot of people, this was unthinkable. I mean, after all, clearly this paper does not have any real value. It took about 400 years for paper, as money, to become accepted broadly. It was a big aberration.

"You think people are freaking out about bitcoin? Imagine how much they freaked out when you told them that now, instead of trading in gold, they would trade in pieces of paper."

2.2.3. Paper to Plastic

Then, about 60 years ago, we saw a new form of money in the form of plastic cards. In fact, the first cards were paper again. In the United States, Diners Club was the first to create a credit card, which was a form of traveler's cheque. Then, people took that and they said, "This isn't money. Why don't you give me some of the good old paper money that I know?" That was another big transformation in money.

2.2.4. Plastic to Bitcoin

Now, we have bitcoin. Bitcoin is, in my mind, a pretty radical transformation. It's as radical as the change from precious metals to paper money. Perhaps even more radical. So what is bitcoin? The fundamental issue in describing bitcoin is that if you use references to our existing experience, that experience is based on thousands of years of understanding what money is in a very physical form. Now, we're trying to explain a form of money that is completely abstract. "It's a token that represents acceptance in a network, a network-centric form of money." But that doesn't even begin to describe what this thing is.

One of the most common misunderstandings, when I try to describe bitcoin, is that people think that it's simply a payment system, that bitcoin is simply a form of digitization of money. It's digital money. Great. Well, that's kind of pointless because we already have digital money. All of you use digital money every day, long before bitcoin came along. You have bank accounts. Those bank accounts have digital ledgers. You use those bank accounts to send payments electronically. That's digital money.

"Bitcoin is a fundamental transformation of the technology of money."

Bitcoin isn't just digital money. Bitcoin is a fundamental transformation of the technology of money. It's difficult to grasp because it's so different from everything we've known before. So, I will take a different stab at it. I want to take a look at network architecture for a second.

2.3. Moving to a Network-Centric, Protocol-Based Era

Bitcoin is not happening in a vacuum. It's happening at a moment in history when we're seeing a transformation of many fundamental social institutions. That transformation is the great network-centric era.

For centuries, social institutions were organized around hierarchical organizations: institutions, democracy, banking, education. All of our social interactions were organized by appeal to authority in these hierarchies, these bureaucracies of people. But something happened with the invention of the internet. We started seeing more and more of these social institutions changing from systems that were closed, opaque, unaccountable hierarchical complexes with their own rules, into platforms. We started seeing the introduction of systems that have interfaces, API's that we can access, where information can flow in and out of the organization. So, we move from institutions to platforms.

Then, we start seeing an even more important transformation, when we move from platforms to protocols. The interesting thing about the change between a platform and a protocol is, when you have a protocol there is no central appeal. TCP/IP doesn't work in reference to a service provider. TCP/IP works without context everywhere in the world. You don't have to sign up for an account to use TCP/IP; you just have to use the language. Once you move from a platform to a language, it opens up all of these possibilities.

"Bitcoin is the first network-centric, protocol-based form of money. That means it exists without reference to an institutional or platform context."

Bitcoin is the first network-centric, protocol-based form of money. That means it exists without reference to an institutional or platform context. I'll get back to that in a second, this is a really important point.

2.3.1. Peer-to-Peer Architecture

We say that bitcoin is peer-to-peer money. What does that mean? It refers to an architecture used in terms of computer science or networking or distributed systems to describe the relationship between participants and a system. The architecture of bitcoin is peer-to-peer because every participant in the network speaks the bitcoin protocol on an equal level. There are no special bitcoin nodes; all nodes are the same.

Peer-to-peer means that when you send out a transaction to the network, every peer treats it the same. It has no context inside the peer's system other than what it gets from the network. An interesting issue in distributed systems is this issue of context and state. If you log in to Facebook and you have an account with Facebook, you're not using a protocol. All of the state is controlled by Facebook. You have a login session and all of the data is held by them. We call that architecture *client-server*. Bitcoin is different because it's peer-to-peer, just like email or TCP/IP.

2.3.2. Client-Server Architecture

We are reluctant to discuss money. In fact, it's shocking that in almost all countries, money is not part of the education system. Five-year-olds have great questions about money. Most parents find it almost impossible to answer these questions. "What is money, Mommy? How does money work? Why do we not have more of it? Why can't everyone have more of it?" You don't say, "Suzy, go back to your room and study inflation, like a good girl, and don't come back until you understand the answer to those questions!"

We don't discuss money. It's interesting — we use a technology as a foundation of almost every aspect of social interaction, and yet it is a completely taboo subject. We all pretend that we don't particularly care about money, at least not intrinsically. We have higher goals and aspirations. We use it in everyday experience but we don't really talk about it. It's a dirty topic.

I think the architecture has something to do with it. Before bitcoin, the previous iteration of money — when money started being issued in exchange for precious metals stored in a vault — what that represented was a form of debt. That's a really important concept to understand because it colors our discussion.

"Before bitcoin, the previous iteration of money — when money started being issued in exchange for precious metals stored in a vault — what that represented was a form of debt."

How many of you have money in a bank? None of you has money in a bank. Do you store physical money in a safe deposit box? If so, maybe then you could say you have money in a bank. The rest of you have loaned your money to a bank. For the privilege of loaning your money to a bank, you will be paid the amazing interest rate of 0.00001 percent per year. Your bank will take that money, turn around, and loan it to the people standing next to you for 24.99 percent APR.

"This is a client-server relationship. Because that money only exists as a form of debt in a ledger that you do not control. A ledger that is stored by a server, and you are simply a client. In fact, you have no control over it at all."

This is a client-server relationship. Because that money only exists as a form of debt in a ledger that you do not control. A ledger that is stored by a server, and you are simply a client. In fact, you have no control over it at all. You don't even have basic interfaces to that money unless that interface is mediated by the server. That's what a client-server architecture does.

2.3.3. Master-Slave Architecture

We have another term in distributed systems that describes a particular form of client-server architecture, where the secondary party only has a weak copy that isn't really meaningful. We call that a *master-slave architecture*. If you think of the previous iteration of money as a master-slave architecture, you have to ask an uncomfortable question: Who is the slave? Because in a system of debt, one of the two parties is always the slave.

"...in a system of debt, one of the two parties is always the slave."

You are the client. You are not the server. The server doesn't really serve you; they serve themselves because they're the master. That is the architecture of money we live in. That is the architecture of money we use in our civilization: an architecture of money where you have no control; an architecture of money where every interaction is mediated by a third party that has absolute control over that money.

Today, if you go to an ATM machine and you put in your card, the bank may decide to give you your money. One day—as the people of Cyprus, Greece, Venezuela, Argentina, Bolivia, Brazil, and a list of hundreds of countries over the last several decades and even centuries have discovered—one day, you go to the bank and the bank does not want to give you the money, because they don't have to. That's the essence of a master-slave relationship.

"Bitcoin is fundamentally different because in bitcoin, you don't owe anyone anything and no one owes you anything. It's not a system based on debt."

Bitcoin is fundamentally different because in bitcoin, you don't owe anyone anything and no one owes you anything. It's not a system based on debt. It's a system based on ownership of this abstract token. Absolute ownership. We have an expression in the United States, which is "possession is nine-tenths of the law." In bitcoin, possession is ten-tenths of the law. If you control the bitcoin keys, it's your bitcoin. If you don't control the bitcoin keys, it's not your bitcoin. You're back to a master-slave relationship.

"In bitcoin, possession is ten-tenths of the law. If you control the bitcoin keys, it's your bitcoin. If you don't control the bitcoin keys, it's not your bitcoin."

2.4. Bitcoin, a Fundamental Transformation of Money

Bitcoin represents a fundamental transformation of money. An invention that changes the oldest technology we have in civilization. That changes it radically and disruptively by changing the fundamental architecture into one where every participant is equal. Where transaction has no state or context other than obeying the consensus rules of the network that no one controls. Where your money is yours. You control it absolutely through the application of digital signatures, and no one can censor it, no one can seize it, no one can freeze it. No one can tell you what to do or what not to do with your money.

It is a system of money that is simultaneously, absolutely transnational and borderless. We've never had a system of money like that. It's a system of money that transmits at the speed of light, one that anyone in the world can participate in with a device as simple as a text-messaging phone.

This represents a technological innovation that is terrifying to a lot of people because it is such a fundamental transformation of money. What they will tell you is that they're worried. They're very worried. They're worried that criminals will use bitcoin. But the truth is that they're far more terrified that all of the rest of us will.

Thank you.

Chapter 3. Privacy, Identity, Surveillance and Money

Barcelona Bitcoin Meetup at FabLab; Barcelona, Spain; March 2016

Video Link: <https://www.youtube.com/watch?v=Vcvl5piGIYg>

Today, I'm going to talk about the concepts of neutrality, decentralization, privacy, and what makes bitcoin so special. You've heard me talk a lot about bitcoin. When I use the word *bitcoin*, I am not talking about the currency. I am talking about a broader concept: the concept of completely decentralized, network-based, flat networks for providing trusted applications. If you happen to have a completely decentralized flat network that could provide trusted applications, the most logical first application is currency. But currency is just the first app.

3.1. Banking: Liberator to Limiter

We are restructuring society by rebuilding institutions. Traditionally, our institutions have been hierarchical in design. This was an invention of industrialization, an 18th-century concept to allow people to organize and communicate at a larger scale. It was very effective at breaking the monopolies of kings and feudal systems. It has now run its course.

Sometimes people ask me what my political positions are, and it's very difficult to explain, but one word captures it, I think: I am a *disruptarian*. What that means is that every 30 or 40 years at least, things that have settled need to be disrupted. Because as they settle, power accumulates, they become centralized, and with centralized power, corruption happens. This isn't a new concept. My ancestors—I come from Greece—figured out that corruption happens in systems of power, and absolute power produces absolute corruption. There is no more absolute power than the power over money.

"Every 30 or 40 years at least, things that have settled need to be disrupted. Because as they settle, power accumulates, they become centralized, and with centralized power, corruption happens. There is no more absolute power than the power over money."

We live in a world where banking was once a great liberator. It was an invention that moved finance from the realm of kings to the realm of everyday people. That system liberated billions of people. And then it got concentrated, it acquired power, and the power led to corruption. What we're left with today is not a liberating system, and it's time to disrupt it. Bitcoin is one of the things that will greatly disrupt centralization of power. Why is that?

3.2. Negative Outcomes by Design, Not Intent

One of the things that interests me as a computer scientist working in distributed systems is the architecture of systems. Architecture is a great topic for this city. The architecture of systems is what ultimately produces the outcomes.

I've worked with a lot of bankers. They're nice people. They try to feed their family, pay their mortgage, keep a steady job. Among them, there are a few sociopaths who inevitably rise to the highest positions of power because sociopathy is an advantage in hierarchical systems. But most of the problems with traditional concentration of power in money has nothing to do with the people being evil. It has to do with the fact that these institutions — through their shape, through their architecture — produce outcomes that are not good. They produce outcomes that are not egalitarian. They produce outcomes that are restrictive. They start to express nativism, nationalism, tribalism, class structure, and all of these things make the world a smaller place.

3.3. Communications Expanding While Access to Banking Is Declining

In fact, over the last 15 years, we've seen the internet become an enormous power for the decentralization of communications. It has been a very liberating force. But if you look at economic inclusion and how banking works, we haven't expanded opportunity. We haven't expanded access. In fact, we're now regressing. Economic inclusion is decreasing.

The reason it's decreasing is because these isolated structures of finance, their very architecture, raise walls: national borders, class structures, and differences in how your money and your commerce are treated. We live in a world that is increasingly global and interconnected. There is even an emergent global culture through the internet. And yet our financial systems are parochial, insular, and they're separated.

"We live in a world that is increasingly global and interconnected, and yet our financial systems are parochial, insular, and separated."

If you look at it from a network perspective, there are systems of money for transmitting small amounts and systems of money for transmitting large amounts. Systems of money for consumer payments, systems of money for business-to-business payments. All of these are separated geographically based on borders, legal jurisdictions, nation-states. What the structure produces is separation. It means that, as people, we are less and less free to transact with the rest of the world. Geopolitics is affecting finance in a serious way because the combination of state and money produces toxic results.

And we're about to disrupt all that.

3.4. New Architecture, New Access

What bitcoin's architecture gives us is a new way of organizing the world, exactly the same way that the internet flattened access to communication and made every system that connects to it an equal peer. If I have an IP address, my packets are treated no differently than the packets of anybody else on the network. For the most part, that gives voice to everyone. It gives everyone the power of the printing press on a global scale. Bitcoin will do the same by giving everyone the power of banking on a global scale.

"What bitcoin's architecture gives us is a new way of organizing the world, exactly the same way that the internet flattened access to communication and made every system that connects to it an equal peer."

Think of it like desktop banking. In the way desktop printing, desktop publishing and websites changed communications, desktop banking — individually controlled banking with all of the power of the largest bank in the world — will create disruption.

Imagine a world where every person has the ability not only to execute transactions but also to create complex financial systems and instruments without asking for anyone's permission. Simply by connecting to the network, anyone can start a new application. Centralized systems can't do that.

In a centralized system, the further out you are, the less control you have. The closer you get to the system, and the farther you move up the hierarchy, the more controlled, the more limited the access is. But not with bitcoin. With systems like bitcoin, every node on the network has equal access to all of the financial services. In a centralized system, if you want to build a new application, you must first ask permission. And then permission is only granted if that application can apply to a very large population and be profitable.

On the internet or on bitcoin, all that is needed to start an application is two nodes, two people, two systems. They can start communicating, construct their own protocols, their own systems, and that application with only two people using it is just as valid as every other application on the network.

3.5. Net Neutrality and Non-Discrimination

When you look at the internet, the fundamental misunderstanding is that people think that the power of the internet comes from the ability to transmit information fast. But the real power of the internet comes from net neutrality. Net neutrality is the concept that the internet does not discriminate based on source, destination or content.

"Bitcoin is the first financial network that exhibits neutrality."

Bitcoin is the first financial network that exhibits neutrality. In a bitcoin transaction, the network doesn't care about the source, the destination, the amount or what type of financial application it's supporting. The only relevant question is, did you pay a sufficient fee to use the network resources? And if you did, your application is valuable.

3.5.1. There Are No Spam Transactions in Bitcoin

We have an interesting conversation happening in bitcoin right now. Perhaps some of you have heard the term “spam transactions.” What is a spam transaction? What does it mean for a transaction to be “spam”? I think that term is meaningless because to decide which transactions are spam and which are not, you’re making a top-down judgment. You’re imposing, in the architecture, the choices of which applications are legitimate. Then the question is legitimate to whom? The end user? There is no such thing as a spam transaction simply because if a transaction carries enough fee, that means that the sender of that transaction felt it was valuable enough to transmit—and therefore, it is a legitimate transaction. This replaces the concepts of control and content by making decisions about what is good, what is bad, what is legitimate, what is illegitimate, what is a valuable application, what is not a valuable application, with a simple market mechanism. If you paid essentially a tiny fee for your transaction, then because of the democratization of finance, your transaction is valuable and is not spam.

3.6. Network-Centric Money

Starting in the 1970s, we have seen the world begin to adopt digital currencies. When people call bitcoin a “digital currency,” they’re missing the point. The euro is a digital currency, the US dollar is a digital currency. Less than 8 percent of these currencies exist in physical form; the rest is bits on ledgers. But the fundamental difference is that these ledgers are controlled by centralized organizations, whereas in bitcoin, they’re not. Bitcoin has a decentralized network, an open network.

"Bitcoin isn't a digital currency. It's a cryptocurrency. It's a network-centric money."

Bitcoin isn't a digital currency. It's a cryptocurrency. It's a network-centric money. I really like the idea of a network-centric money. A network that allows you to replace trust in institutions, trust in hierarchies, with trust on the network. The network acting as a massively diffuse arbiter of truth, resolving any disagreements about transactions and security in a way where no one has control.

3.7. Dreaming of Totalitarian Control over All Financial Transactions

Starting in the 1970s, our currencies began to be digital, but this is not the same “digital” as bitcoin. This started a dream for governments, the dream of being able one day to control every financial transaction of every human being on the planet in a way that everything was visible to the power structures. Where privacy dies. Where the ability to make a transaction immediately puts you under the lens of systems that surveil you. We have been creating a system of global financial surveillance. A system of totalitarian financial surveillance throughout the world.

"This started a dream for governments, the dream of being able one day to control every financial transaction of every human being on the planet in a way that everything was visible to the power structures. Where privacy dies."

That system, which requires identification and credit checking and limited access, is responsible for the fact that economic inclusion is regressing. It is responsible for the fact that 2 1/2 billion people have absolutely no access to banking. That's just the heads of household, not counting their families. That's not counting people who have limited access to banking in a single currency within a single border. If you count all of them, it's billions upon billions.

3.7.1. Censorship of Financial Transactions

As a member of the privileged elite of the developed world, I have the ability to open a brokerage account in 24 hours, electronically. And within 24 hours, I can be trading in yen on the Tokyo stock market. I can be sending and receiving money anywhere in the world without really any limits. All I have to do is sacrifice my privacy and my freedom.

Because while I can do all of those things and they're very powerful, there are some things I can't do. I am not talking about buying drugs. That's not really that interesting. What I am talking about are simple things — for example, donating to an activist organization like WikiLeaks. A few years ago, WikiLeaks was completely cut off from the world's financial system simply with extrajudicial pressure applied on the few major payment providers: Visa, MasterCard, the banking transfer system, PayPal, etc. Without any legal process, without any conviction, and perhaps, in my opinion, without absolutely any crime other than revealing the truth of crime, WikiLeaks was cut off from the world's financial system. This is now happening not just to activist organizations; it's happening to entire countries.

The dream of nation-states, to create a totalitarian financial system, died on January 3rd, 2009, with the invention of bitcoin and the mining of the genesis block.

"The dream of nation-states, to create a totalitarian financial system, died on January 3rd, 2009, with the invention of bitcoin and the mining of the genesis block."

3.7.2. Network-Centric Money Is Censorship Resistant

Bitcoin is *censorship-resistant*. You may have heard this term. You cannot control where money is transmitted in bitcoin. It's not attached to identities or geography. In bitcoin, surveillance of everyone is not possible. In bitcoin, censorship resistance is an artifact that is created by neutrality, the architecture of a flat network without borders. The architecture of neutrality that doesn't ascribe any meaning to source, destination or value, is what creates censorship resistance.

3.8. Sousveillance, Not Surveillance

Privacy is very important but it's a term that often has very deep political meaning. I like to juxtapose it to another term, *secrecy*. What is the difference between privacy and secrecy? Ultimately, and practically in today's vocabulary, privacy is the right of billions of individuals to not be surveilled. Secrecy is the power of the very few to escape accountability, to have no transparency.

We live in a world where every individual transaction you do through the financial system is cataloged, analyzed, and transmitted to intelligence services all around the world that collaborate, and yet we have no idea what our governments do with money. The financial systems of the powerful are completely opaque. Our transactions are completely visible through this system of surveillance. This world is upside down. Bitcoin rights it.

Privacy is a human right and secrecy is a privilege of power, and we need to be in a world where we have complete, ultimate, strong privacy for the billions of people. Because that is a human right, because that is a cornerstone of the freedoms of expression, association, political speech, and all of the other freedoms that are very much attached to privacy. We need to live in a world where secrecy is fickle and easily pierced, where power has to face accountability because they are under the spotlight of transparency. We need to flip the system upside down.

"Privacy is a human right. Secrecy is a privilege of power. We need to live in a world where secrecy is fickle and easily pierced, where power has to face accountability because they are under the spotlight of transparency."

One of my favorite words is a French word: *sousveillance*. It is the opposite of surveillance. Surveillance means to look from above; sousveillance means to look from below. In their dream of nation-states controlling all of our financial futures, they made one major miscalculation. It's a hell of a lot harder for a few hundred thousand people to watch 7 1/2 billion. But what do you think happens when 7 1/2 billion of us stare back? When the panopticon turns around. When our financial systems, our communication systems, are private, and secrecy is an illusion that can't be sustained. When crimes committed in the names of states and powerful corporations are vulnerable to hackers and whistleblowers and leakers. When everything eventually comes out. We have a great advantage because the natural balance of the system is one in which individuals can have privacy but the powerful cannot have secrecy anymore. Bitcoin is one of the first steps in that.

"We have a great advantage because the natural balance of the system is one in which individuals can have privacy but the powerful cannot have secrecy anymore. Bitcoin is one of the first steps in that."

3.9. Banks for Everyone

The ability to transact across borders means that we will now be able to extend financial services to billions of people who have no access. Not through complicated technology necessarily. Sometimes I speak to various regional banks, the ones that are not afraid of bitcoin. They tell me things like 80 percent of our population is a hundred miles from the nearest bank branch and we can't serve them. In one case, they said a hundred miles by canoe. I'll let you guess which country that was. Yet, even in the remotest places on earth, now there is a cell-phone tower. Even in the poorest places on Earth, we often see a little solar panel on a little hut that feeds a Nokia 1000 phone, the most produced device in the history of manufacturing, billions of them have shipped. We can turn every one of those into, not a bank account, but a bank.

"I don't have a Swiss bank account in my pocket. I have a Swiss bank."

Two weeks ago, President Obama at South by Southwest did a presentation and he talked about our privacy. He said, "If we can't unlock the phones, that means that everyone has a Swiss bank account in their pocket." That is not entirely accurate. I don't have a Swiss bank account in my pocket. I have a Swiss bank, with the ability to generate 2 billion addresses off a single seed and use a different address for every transaction. That bank is completely encrypted, so even if you do unlock the phone, I still have access to my bank. That represents the cognitive dissonance between the powers of centralized secrecy and the power of privacy as a human right that we now have within our grasp. If you think this is going to be easy or that it's going to be without struggle, you're very mistaken.

3.10. Bitcoin, the Zombie of Currencies

If you read anything about bitcoin, you'll see the very same things that they said about the internet in the early '90s. It is a haven for pedophiles, terrorists, drug dealers, and criminals. How many of you in this room have bitcoin? How many of you in this room are terrorists, pedophiles, drug dealers or criminals?

You see the thing about bitcoin is while they push this story, every now and then someone who has never heard of bitcoin notices two important things. One, it's still not dead, which is always surprising because every two or three months there is an article that says it's dead. That's great marketing. Because every time someone hears it's dead and three months later they hear it's still not dead, they think, "Huh, this thing really tends to survive." I call bitcoin "the internet of money," but perhaps we should call it "the zombie of currencies." It is the currency that is the undead.

"I call bitcoin "the internet of money," but perhaps we should call it "the zombie of currencies." It is the currency that is the undead."

The issue here is that we're now creating a system that is threatening the largest industry in the world, and that is finance. They are going to object. They are going to push back, and they're going to use the most common and effective emotional tactic there is, which is fear. They will treat you in such a way as if you are idiots and try to persuade you that this is something to fear. When people hear that message, maybe the next day they come to one of these meetups and they meet a dentist who owns bitcoin, an architect who owns bitcoin, a taxi driver who uses bitcoin to send money back to their family—normal people who use bitcoin to give themselves financial power and financial freedom. Every time that message is broken by cognitive dissonance, bitcoin wins. All bitcoin really has to do is survive. So far, it's doing pretty well.

3.11. Currencies Evolve

In the new network-centric world, currencies occupy evolutionary niches. They evolve, like species, based on the stimulus they have from their environment. Bitcoin is a dynamic system with software developers that can change it. The question is, in which direction will bitcoin evolve? Which environmental niche will it attempt to fit in? And how will that be affected by the actions of the powerful? If they attack bitcoin, it evolves to defend itself against predators, just like any species. If they attack bitcoin anonymity, it evolves to become more anonymous. If they attack its resilience, it evolves to become more decentralized. In the end, despite all of the messages of fear, bitcoin is the cuddly little bear of currencies and you do not want to kick it. Because, as in evolution, if you stomp on the little gecko, it will evolve until it's a Komodo dragon and then you can't stomp on it.

Sometimes people ask me, "Do you think governments will ban bitcoin? Do you think they will try to regulate it out of existence? Do you think they will attack it with denial-of-service attacks?" The answer is really simple because in network-centric systems—systems that are dynamic and adaptable, systems that exhibit antifragility — attacks cause the system to adapt and evolve and become resistant. Think about this for just a second.

"In network-centric systems, attacks cause the system to adapt, evolve, and become more resistant."

3.11.1. Attacks Build Resistance

I've been involved with the internet since 1989. I remember very clearly, in the early days when lots of articles were written about how the internet was not resilient, could not scale to do voice, was not secure. I remember times when denial-of-service attacks would take down Yahoo, AltaVista, and even Google for hours, sometimes days. What happened between then and now? How many times have you seen Google go down in the last five years? Have people stopped attacking Google? Quite the opposite. Google can now sustain gigabits of denial-of-service anywhere in the world and dynamically reroute. The same applies for all internet applications. The attacks didn't stop. The system became immune because, like a human immune system, if you are exposed to a virus and it doesn't kill you, you evolve resistance, and the next time you're exposed to the virus, it does nothing to you.

Will governments try to ban bitcoin? Regulate bitcoin? Attack bitcoin? They already are. They have been, almost since the beginning, and bitcoin is still getting stronger. It's a system that is under a constant denial-of-service attack, that is on the internet being attacked by hackers, by agents, by other systems, 24 hours a day.

"bitcoin is still getting stronger. It's a system that is under a constant denial-of-service attack, that is on the internet being attacked by hackers, by agents, by other systems, 24 hours a day."

In security, we have a really funny term, which is a *honeypot*. A honeypot is a system that is designed to attract hackers. What bigger honeypot could you have than a financial network that has \$6 billion on it? If you hack bitcoin, there is a \$6 billion reward for you finding a way to hack it. No one has collected that reward yet, and it's not because they haven't been trying. They've been trying nonstop. But systems like bitcoin are resilient.

3.12. Welcome to the Future of Money

Remember that what we're doing here is not a currency. It is a reworking of the societal systems of organization that have failed us. The 18th-century systems of hierarchies that do not scale to a global, interconnected world are being replaced by network-centric, flat architectures—whether that's the internet or any of the applications running on top of it or bitcoin itself. Currency is just the first app. When you have a network that can provide you with neutral trust, you can build myriads of applications on top, and you don't have to ask for permission.

Bitcoin is much more than currency. When I say that bitcoin is “the internet of money,” the emphasis is not on “money”; the emphasis is on *internet*. Welcome to the future of money.

Thank you.

Chapter 4. Innovators, Disruptors, Misfits, and Bitcoin

Maker Faire; Henry Ford Museum, Detroit Michigan; July 2014

Video Link: <https://www.youtube.com/watch?v=LeclUjKm408>

Just before this presentation began, attendees viewed a video presented by the museum about the history of the automobile. That is the video referenced throughout this talk.

Good morning. Now that was a fun video, wasn't it? About a month ago, I sold my car for bitcoin. That was an interesting experience, a whole new world. How many here have bitcoin? Of those who don't, how many of you have heard of bitcoin? *95% of audience has heard of bitcoin.* Anybody who has not heard of bitcoin? Okay, great, this is going to be a lot easier than I thought.

4.1. Recognizing Innovation

Bitcoin is the internet of money, but it's a lot more than that. For this audience in particular and for the people who are here at the Maker Faire, I want to talk about bitcoin from the perspective of the misfits, the weirdos, the freaks. The people who refuse to think the way everybody else thinks. The people who see a half-working, elegant technology and don't look at the *half-working*; they look at the *elegant* side. They recognize innovation. And they recognize innovation, not just a few months or a few years before others, but sometimes a decade before others. Those are the kinds of people that come to Maker Faire. And so it's a great place to start talking about bitcoin.

Bitcoin is unexpected. Bitcoin is not money as we know it. Bitcoin should not have happened. Bitcoin really has no possibility of success. It can't possibly work. It's one of those things that does not work in theory, but it works in practice. Like Wikipedia. Like Linux. Like the internet. Weird ideas made by people with ponytails and neckbeards. Weirdos nobody really trusts.

"Bitcoin is unexpected. Bitcoin is not money as we know it. Bitcoin should not have happened. Bitcoin really has no possibility of success. It can't possibly work. It's one of those things that does not work in theory, but it works in practice. Like Wikipedia. Like Linux. Like the internet."

Bitcoin succeeds because it works. As a technology, it's elegant. I want to talk about that spirit of the misfit. About walking into an industry boardroom saying, "You know what? We're about to change everything," and being laughed out of the room. Then, keeping on and going on, until, in fact, they change everything. This happens in technology all the time. We just forget about it. We ignore it. We rewrite the history in glowing terms.

4.2. The Dangers of Automobiles, Electricity, and Bitcoin

We just watched a video about the early automobile. Do you know what the media said about the early automobile? They ridiculed cars. They mocked cars. Cars were slower than horses. Cars broke down all the time. Cars needed expensive gasoline that you couldn't find anywhere. They required enormous amounts of infrastructure to work. The media focused on the part of the story that sold the most papers: car accidents, pedestrians mangled by cars. For more than two decades from the first cars, the story was that of infernal, disgusting, dirty, noisy machines that were far inferior to horses, that couldn't go anywhere, that only weirdos would use, and that, most of the time, killed the occupants and everyone who came anywhere near them.

"For more than two decades from the first cars, the story was that of infernal, disgusting, dirty, noisy machines that were far inferior to horses, that couldn't go anywhere, that only weirdos would use, and that, most of the time, killed the occupants and everyone who came anywhere near them."

This hysteria got so bad that in 1896 in the UK, they passed a law called the Red Flag Act. The Red Flag Act required that any operator of a vehicle have three crew members on staff: a driver, an engineer, and a flagman. The driver would operate the vehicle, the engineer would supervise that operation (think railroads), and the flagman would carry a red flag and run 100 yards ahead of the car to warn pedestrians of the imminent arrival of an infernal death machine that was going to mow them down.

Guess what happened to the UK? They lost the automobile-industry race because they saw that technology and, instead of seeing potential, they allowed fear to define their reaction. They created an environment where a car could not do the things that a car can do. If you make a car go as slow as the pedestrian who's running ahead of it with a red flag, you lose all of the advantages of a car. If a car requires a three-person crew to operate, you lose the advantages of a car. They tried to take the car and understand it from the perspective of railroads and horses. They failed. They lost the race.

What you didn't see in this video is that until that time, they were winning. The first really practical cars were built in England. They had already won the race in the Industrial Revolution with the steam engine. At that time, England was a powerhouse of industrial innovation. They were winning, until they decided that this dirty machine should be confined to a very limited space and set of rules. They killed the goose. No more golden eggs for them.

"The first really practical cars were built in England... At that time, England was a powerhouse of industrial innovation. They were winning, until they decided that this dirty machine should be confined to a very limited space and set of rules."

That is instructive because this happens again and again in technology. When electricity was first domesticated and people started electrifying their homes, do you think the media announced, "This is brilliant! Edison's a genius! This is going to change the world!"? No. What they said was that this was dangerous technology that would burn down people's homes. They ran story after story after story about people getting electrocuted, about homes burning down.

"When electricity was first domesticated and people started electrifying their homes, do you think the media announced, 'This is brilliant! Edison's a genius! This is going to change the world!'? No. What they said was that this was dangerous technology that would burn down people's homes."

Of course, you couldn't really use electricity because it required a complete overhaul of your house. You had to put wires in your house, the wires that would burn it down. You'd have to buy special devices to connect to these wires, just before your house burned down. Only the rich could afford it. Clearly, this was a technology that was just an affectation of the rich. It was just a plaything with no practical value.

The mayor of Paris, during the World's Fair of 1900, said, "After the fair is over, this fad of electricity will be forgotten as quickly as the lights turn off." Famous last words are very common in technology, words that in retrospect look ridiculous. Like the head of IBM who once said, "I foresee a need for no more than five computers worldwide." Like the people who said that the telephone would never succeed.

"Famous last words are very common in technology, words that in retrospect look ridiculous."

Can you guess what people are saying about bitcoin? They're telling you that it is a technology that is weird and complicated. A technology that caters to misfits, drug dealers, degenerates, pornographers, terrorists, thieves, swindlers. I don't see any of those people in this room but we better be careful just in case they show up.

Of course, they're wrong. Bitcoin is none of those things. Bitcoin is simply a technology. As a technology, often the first use it finds is in the hands of criminals. The first cars were used as getaway vehicles. The first telephones were used to plot conspiracy. The first telegrams were used to run long-distance mail-fraud schemes and Ponzi schemes. The first forms of electricity were used to run medical hoaxes and scam people. These things always happen with a new technology, and they happen with bitcoin, too.

"Bitcoin is simply a technology. As a technology, often the first use it finds is in the hands of criminals. The first cars were used as getaway vehicles... Criminals use the most cutting-edge technology because they operate in an environment with very high profit margins and very high risk."

Why do you think criminals use technology like that? We could be moralistic about it and look at the actual reasons. Criminals use the most cutting-edge technology because they operate in an environment with very high profit margins and very high risk. In that environment, competition is fierce. Using the latest technology if you're already taking enormous risks isn't that big of a deal. And if you win, it gives you an enormous advantage. Throughout history, the most amazing technology is adopted by criminals first. I don't think that's necessarily what we want to put on the bitcoin marketing plan, but it's interesting to look at what criminals do and how that ends up being mainstream technology a decade later. There's a certain dynamic there.

Bitcoin is already way past its early stage and is no longer the purview of criminals. In fact, arguably it really wasn't in the first place, despite what the media said. Now, bitcoin is hitting the mainstream and things are changing very rapidly.

"With bitcoin as a technology, something very exciting is happening. Something is going to shake up our financial and banking system as much as cars shook up the horse industry, as much as oil shook up the whaling industry, as much as electricity shook up the wood stove industry."

Today I'm going to talk about bitcoin as a technology because something very exciting is happening. Something is going to shake up our financial and banking system as much as cars shook up the horse industry, as much as oil shook up the whaling industry, as much as electricity shook up the wood stove industry. Banking is about to be disrupted. Arguably, it's already being disrupted. In fact, by the time they figure out how serious this destruction already is, the game's already over. That's usually the case.

4.3. Incumbent Reactions to Innovation

When established, entrenched industries first see a new disruptive technology, they ignore it because it can't possibly pose a threat. From the benefit of incumbency, from the high perch of an established monopolistic business, these threats look like children playing around. To JPMorgan Chase, bitcoin is like a lemonade stand trying to take on Walmart. If the technology continues to exist, then they go into the next phase where they start mocking the technology. They suddenly see it everywhere and they start making jokes about it. So, just like with the automobile, the first people who bought cars were mocked. They were shown always on their knees with a spanner, trying to fix their machine that had broken down again. That was the image of an automobile owner for the first years.

While they mock it, bitcoin continues to grow and improve. After a while, you see a change. At first, some of the incumbents in the industry say, "Hey, maybe we need to experiment with this. Maybe we need to start looking at this." Then there's a stampede because suddenly they realize *this is going to change our industry forever*.

By that time, it's too late. By that time, they're Kodak: going from number one in the world to, within three years, losing a \$12 billion industry right out from under their feet to a company they had never even heard of before. A company that didn't even make cameras. Do you know who destroyed Kodak? A little Finnish company they had never heard of called Nokia. A company that didn't make cameras—until they did. Within three years they made half a billion cameras and destroyed Kodak. Tower Records dominated the music industry. Within four years they disappeared. Why? Because MP3s gave people choice.

IBM used to be the most unshakable company in computers. They guaranteed quality. In fact, buying anything but IBM was a sure sign that you were a loser. Then Linux happened. Linux shook IBM to the core because it subverted the very basic idea that in order to deliver quality engineering, in order to deliver the best computers possible for the serious work of banking, engineering, and government operations, you needed IBM. You needed a closed, controlled, carefully organized system built by serious Ph.D. engineers.

Back in 1992 when Linus Torvalds said, "I'm going to build an operating system in my dorm room because I can't afford to buy an operating system," that idea seemed completely preposterous. Operating systems were enormous edifices of complexity that took thousands of engineers to build. Linus Torvalds started

simple; he started building an operating system. Six years later, Linux had started dominating the computing industry and Sun Microsystems was beginning to feel the pain. Eight years later, Sun Microsystems was heading into bankruptcy, HP was getting bought, their computer division was shutting down, and IBM stepped out of the personal-computing business.

Now, 80 percent of the cell phones on the planet run Android — which, by the way, is Linux. The servers they connect to run Linux. The banks we use run Linux. The entertainment systems we use run Linux. The cars we drive run Linux. You can always tell if they stop running Linux: the little blue screen that greets you that says, *Bleh. Sorry. Crashed. Wrong choice of operating system.* You get into a plane, the entertainment system boots up, it's running Linux. If you said to an IBM engineer 15 years ago, "You are about to be destroyed by an operating system built by a Finnish student in their dorm," they would have laughed at you.

"If you said to an IBM engineer 15 years ago, 'You are about to be destroyed by an operating system built by a Finnish student in their dorm,' they would have laughed at you."

Here we are today, and bitcoin is taking on the entire banking system, the most powerful industry in the world. Guess what? Bitcoin's going to win. It's going to win for a very simple reason. It's not just going to win because it's better. It's not just going to win because the banking system is run by gangsters, crooks, and some of the most immoral empty suits in the world. It's not just going to win because the banking system has spent the last 50 years delivering just two consumer innovations — ATMs and credit cards — and then spent the rest of the time trying to figure out how to fleece you. It's going to win because it's open. In a world of tinkers, of experimenters, of makers, open wins. The reason it wins is that it allows innovation to flourish at the edges.

"Bitcoin is going to win because it's open. In a world of tinkers, of experimenters, of makers, open wins. The reason it wins is that it allows innovation to flourish at the edges."

4.4. Open Innovation and Opt-In Systems

Let me explain what I mean by that. Every single financial system in the world has a security and trust model that requires excluding bad actors. I can't connect to the Visa network and program it because doing so would endanger the security of the Visa network. I can't connect to the SWIFT network, the worldwide interbank wire transfer network, because doing so would endanger the security of that network. All of these networks are designed to be closed because their primary security relies on access control. Very carefully vetting every single person who has access and touches the code. Very carefully vetting all of the applications that run on that system, because if they allow one bad actor into the heart of the system, that security is gone. That one bad actor can take over and do whatever they want. Of course, in 2008 we discovered that the bad actors owned the banks. And they did take over. They destroyed millions of homeowners, millions of retirees, and millions of savers all around the world with their greed.

"Bitcoin is different because it doesn't depend on access control to remain secure. It depends on a simple mathematical formula of incentives and rewards."

Bitcoin is different. The reason it's different is not because we've suddenly found the most honest people in the world. Or because there are no quirks in bitcoin. Or because the network doesn't get attacked. Bitcoin is different because there are plenty of crooks in bitcoin — the network gets attacked all the time — but it doesn't depend on access control to remain secure. It depends on a simple mathematical formula of incentives and rewards. In order to participate in the bitcoin network and secure the network as a miner, which is a special function in bitcoin, you have to use a lot of computing power and spend a lot of electricity. If you win that competition, you get bitcoin as a reward. That simple equation creates a system of incentives where it's far better to play *with* the rules than against the rules. It's game theory. It's like a giant game of Sudoku.

If you look at that as a computer scientist, or even more as a banker, you say, "That can't possibly work. What do you mean it's a giant game of Sudoku and everybody is competing against each other? That's not the basis of a security system. That would bring chaos." It's kind of like "What do you mean it's an encyclopedia that anyone can edit? That would bring chaos" — said the Encyclopedia Britannica. If you're under 40, you've never heard of it.

Bitcoin is a completely open network. Anyone can connect to it. You can write an application right now, connect to the bitcoin network, and teach it to do

something new. You can write a new financial service. You can write a new financial instrument. When you do so, you don't have to identify yourself to the network, you don't have to get permission from anyone. You don't have to be vetted. You don't have to be secured. The network doesn't fear you because its security doesn't depend on keeping bad actors out. In fact, bitcoin works fine with plenty of bad actors right in the core of the system because there is no core of the system; there is no center. It's a completely decentralized system. What happens when you create a network where open access to financial services is possible? Where, for the first time in history, anyone can connect and write an application?

"Bitcoin is the internet of money, and currency is just the first application."

Bitcoin isn't currency. That's a really important thing to realize. Currency is an app that runs on the bitcoin network. Bitcoin is the internet of money, and currency is just the first application. Today, there are a thousand companies writing the next app. Those companies are hiring tens of thousands of people in one of the most vibrant industries we have seen in the last two decades. In 2014, bitcoin startups will receive more than \$250 million of investment. What's remarkable about that is that it's faster than the rate of investment in the internet in 1995. We are ahead of the curve. Bitcoin is growing faster than Twitter did in the first three years. Bitcoin is growing faster than Facebook grew in the first few years. The reason for that is because every misfit, weirdo, freak, or programmer from anywhere in the world can now connect to bitcoin without asking anyone's permission and take their weirdo misfit idea and build a new financial service. A new banking application. A new shopping application. A new escrow application. And that's exactly what people are doing. They are building things that are innovative, new, and brilliant. Things that we've never seen in banking before. Things that wouldn't get past the first planning meeting in your average bank because they'd get shot down.

"When you have these two environments running side by side — the banking environment where everything requires permission, which is most certainly not granted, and a system which is completely open, where innovation happens on the edge without permission — guess who wins. Guess where all of the exciting things happen."

When you have these two environments running side by side — the banking environment where everything requires permission, which is most certainly not granted, and a system which is completely open, where innovation happens at the edge without permission — guess who wins. Guess where all of the exciting things happen. Guess where all of the innovation happens. This is innovation that serves consumers.

"Bitcoin is an opt-in system. You choose to use it. You choose what apps you're going to run. You choose who you're going to interact with. You choose the rules of the game by which you're going to interact. That's why bitcoin is going to win. It delivers innovation that consumers want and need."

No one is sitting on bitcoin and trying to find a way to front run a high-frequency trading algorithm so they can squeeze 3 microcents about four microseconds faster than the other giant bank that's playing with algorithms. No one's trying to find a way to screw you out of your overdraft facility, an innovation that was pioneered by one of the big banks, I think in 2007. They realized that if you were close to the overdraft limit, if instead of running the big transaction first they flipped the order of the transactions and ran a lot of small ones, you'd pay a 25-dollar fee for every one of them, and they could maximize their fees. That's the kind of innovation they were focused on. So, they innovated more ways to screw their customers.

In bitcoin, nobody's doing that kind of innovation. The reason they're not doing that kind of innovation is because in bitcoin you can't force someone to take your app. If you bank with a big bank, it's *their* network, it's their policy, you're using their debit card, playing by their rules, and if you don't like it, you can go elsewhere and discover that they're all the same. Bitcoin is an opt-in system. You choose to use it. You choose what apps you're going to run. You choose who you're going to interact with. You choose the rules of the game by which you're going to interact. If you don't like an app, you don't download it. If you love an app, you download it and you tell all your friends about it. That's why bitcoin is going to win. It delivers innovation that consumers want and need.

4.5. Including 6.5 Billion People in a Global Economy

There's another reason bitcoin will win. There is a massive imbalance that most people here don't notice. Every person in this room has access to a bank account without currency controls. A bank account from which they can buy and sell any currency in the world. A bank account from which they can wire money anywhere in the world. A bank account from which they can access international markets like the Tokyo Stock Exchange or the German stock exchange. A market from which they can access credit and liquidity. Auto loans and mortgages. A bank account which is powerful. That power is available to about a billion people on this planet. A billion people who have access to full-fledged, international, high-liquidity banking facilities.

There are 2 billion people who have no bank accounts at all. There are another 4 billion people who have very limited access to banking. Banking without international currencies, banking without international markets, banking without liquidity. Bitcoin isn't about the 1 billion. Bitcoin is all about the other 6 1/2. The people who are currently cut off from international banking. What do you think happens when you suddenly are able to turn a simple text-messaging phone in the middle of a rural area in Nigeria, connected to a solar panel, into a bank terminal? Into a Western Union remittance terminal? Into an international loan-origination system? A stock market? An IPO engine? At first, nothing, but give it a few years.

We've seen what happens with the development of the cell-phone technology that was deployed in Africa faster than any other technology ever in the history of humanity. We see small villages, where they have no running water, wood fires to cook with, and no electricity — yet there's one little solar panel on top of a mud hut and that solar panel is not there for light. It's there to charge a Nokia 1000 feature phone. That phone gives them weather reports, grain prices at the local market, and connects them to the world. What happens when that phone becomes a bank? Because with bitcoin, it can be a bank. What happens when you connect 6 1/2 billion people to a global economy without any barriers to access?



"What happens when you connect 6 1/2 billion people to a global economy without any barriers to access?"

4.6. Remittances, Impacting Lives around the World

Bitcoin is not a currency. Bitcoin is the internet of money. As a technology, it can bring economic inclusion and empowerment to billions of people in the world. I'll give you one example of a specific application that is going to fundamentally change the lives of more than a billion people in the next five to ten years.

Every day, an immigrant somewhere cashes their paycheck and stands in line to wire 50 percent of that paycheck back to their home country to feed their extended family. Here in the US, 60 million people have no bank accounts, yet they cash their paychecks and send them abroad. Overall in the world, \$550 billion is transmitted every year as remittances from first-world countries. Much of that money is sent to five major destinations: Mexico, India, the Philippines, Indonesia, and China. In some of these places, remittances represent up to 40 percent of the local economy. Sitting on top of that flow of \$550 billion are companies like Western Union, and they take, on average, a cut of 9 percent of every single one of these transactions out of the pockets of the poorest people of the world.

"Imagine what happens when one day one of these immigrants figures out that they can send money back to their home country with bitcoin — not for 15 percent, not 10 percent, not 5 percent, but for 5 cents. Not a percentage; a flat fee."

Imagine what happens when one day one of these immigrants figures out they can do the same thing with bitcoin — not for 15 percent, not 10 percent, not 5 percent, but for 5 cents. Not a percentage; a flat fee. What happens when they can do that? They can, right now. There is a startup company that is handling remittances between the US and the Philippines. They're doing a few million dollars right now, but they're going to start growing. There's \$500 billion sitting behind that dam. When you're an immigrant and you can change your financial future by not paying 9 percent to send money home, imagine what happens if every month, instead of sending 91 dollars home, you send 100 dollars home. That makes a difference. There are a billion people, right now, with access to the internet and feature phones who could use bitcoin as an international wire-transfer service.

4.7. Bitcoin Will Change the World

To sum up, bitcoin is the most exciting technology I have seen. I was on the internet in 1989 as a young kid. I knew it was going to change the world long before most people figured it out. I told everyone around me, "We're going to be shopping on this. We're going to do banking on this thing." People's reactions were quite predictable: "Yeah, Andreas, go do your homework, clean up your room." When I first saw Linux, I said, "Man, this is going to change operating systems forever. IBM is going down." Everybody laughed at me. When I saw the first web browser and the first website, I said, "Every single company in America is going to have a website within a decade." Everyone laughed at me. Well, let me tell you something. I don't know what's going to happen with bitcoin, but I do know that the underlying invention — a system of digital currencies that has no banks, no governments, no central control and is available for anyone to use without asking permission — will change the world.

Thank you.

Chapter 5. Dumb Networks, Innovation, and the Festival of the Commons

O'Reilly Radar Summit; San Francisco, California; January 2015

Video Link: <https://www.youtube.com/watch?v=x8FCRZ0BUCw>

At the beginning of the video, Andreas thanks O'Reilly for agreeing to publish his book, "Mastering Bitcoin", under an open-source license. He thanks the audience and the entire community who helped write the book. It's available on github, Amazon, and at bitcoinbook.info

Today, I want to talk about dumb networks. I want to talk about smart networks. I want to talk about the value of open source when it meets finance. And I want to talk about the festival of the commons.

"Bitcoin is a currency, a network, a technology. And you can't separate these things."

Bitcoin is a currency. Bitcoin is a network. Bitcoin is a technology. And you can't separate these things. A consensus network that bases its value on currency does not work without the currency. You can't just do the blockchain without a valuable currency behind it, and the currency doesn't work without the network. Bitcoin is both. It is the convergence of a participatory consensus network and a global, borderless currency that is fungible, fast, and secure. Today, I want to talk a bit about the bitcoin network and focus on one concept that has some parallels to the early internet.

5.1. Smart vs. Dumb Networks

Bitcoin is not a smart network. Bitcoin is a dumb network. It really is a dumb network. It is a dumb transaction-processing network. It's a dumb network for verifying a very simple scripting language. It doesn't offer a complete range of financial services and products. It doesn't have automation and incredible features built in.

"Bitcoin is simply a dumb network, and that is one of its strongest and most important features."


Bitcoin is simply a dumb network, and that is one of its strongest and most important features. When you design networks, when you architect network systems, one of the most fundamental choices is this: do you make a dumb network that supports smart devices, or do you make a smart network that supports dumb devices?

5.1.1. The Smart Network - Phones

The phone network was a very smart network. The telephone at the end of that network was a very dumb device. If you had a pulse-dialing phone, that thing had maybe four electronic components inside it. It was basically a switch on a wire with a speaker attached to it. You could dial by flicking the hook up and down fast enough.

The phone was a dumb device; it had no intelligence whatsoever. Everything the phone network did was *in* the network. Caller ID was a network feature. Call waiting was a network feature. And if you wanted to make the experience better, you had to upgrade the network but you didn't need to upgrade the device. That was a critical design decision because, at that time, the belief was that smart networks were better because you could deliver these incredible services just by upgrading the network for everyone.

"As a result of smart network design, innovation only happens when a feature is needed by all of the subscribers of the network, when it is compelling enough to disrupt the function of the entire network to upgrade it."

There is one small disadvantage with smart networks. They have to be upgraded from the center out. And that means innovation occurs at the center, by one player, and requires permission. As a result of smart network design, innovation only happens when a feature is needed by all of the subscribers of the network, when it is compelling enough to disrupt the function of the entire network to upgrade it. 

5.1.2. The Dumb Network - Internet

The internet is a dumb network. It's dumb as rocks. All it can do is move data from point A to point B. It doesn't know what that data is. It can't tell the difference between a Skype call and a web page. It doesn't know if the device on the end is a desktop computer or a mobile phone, a vacuum cleaner, a refrigerator, or a car. It doesn't know if that device is powerful or not. If it can do multimedia or not. It doesn't know, it doesn't care.

"In order to run a new application or innovate on a dumb network, all you have to do is add innovation at the edge. Because a dumb network can support smart devices, you don't need to change anything in the network."

In order to run a new application or innovate on a dumb network, all you have to do is add innovation at the edge. Because a dumb network can support smart devices, you don't need to change anything in the network. If you push intelligence to the edge of the network, an application that only has five users can be implemented so long as those five users upgrade their devices to implement that application. The dumb network will transport their data because it doesn't know the difference and it doesn't care.

5.1.3. Bitcoin's Dumb Network

Bitcoin is a dumb network supporting really smart devices, and that is an incredibly powerful concept because bitcoin pushes all of the intelligence to the edge.

It doesn't care if the bitcoin address is the address of a multimillionaire, the address of a central bank, the address of a smart contract, the address of a device, or the address of a human. It doesn't know. It doesn't care if the transaction is carrying lots of money or not much money at all. It doesn't care if the address is in Kuala Lumpur or downtown New York. It doesn't know, it doesn't care.

It moves money from one address to another based on a simple locking script. And that means that if you want to build a new application on top of bitcoin, you can upgrade the devices and you can build an application. You don't need to ask for anyone's permission to innovate. Write the app, launch it on your endpoint, and bitcoin will route it, because bitcoin is a dumb network.

That is the power of innovation on the internet. It's innovation without permission. It's innovation without central approval. It's innovation without a broad network upgrade. And that means bitcoin is not a specific financial network. It's not a financial network for large transactions or small transactions, fast transactions or slow transactions. It's whatever you want to use it for, based upon what you choose to do at the endpoint.

Compare that to the current banking system. The current banking system is built around very smart networks, absolutely and tightly controlled to deliver very specific applications to very dumb endpoints. Even with your most sophisticated online banking, all you can do with your bank is access some HTML that delivers a set of services that they decided they were going to give you. You get no APIs, no ability to run additional applications, no ability to upgrade or innovate or change anything unless the entire network changes to support your new application. The current system has networks for large payments, small payments, or fast payments, but it's not all of the above. Bitcoin is all of those things because it's not discriminating, it's neutral, it doesn't care, it's dumb.

"The current system has networks for large payments, small payments, or fast payments, but it's not all of the above. Bitcoin is all of those things because it's not discriminating, it's neutral, it doesn't care, it's dumb."

The power of pushing intelligence to the edge, of not making decisions in the center, moves the innovation into the hands of its end users and gives those end users the ability to build applications that are so niche that only a handful of

people around the world need them. And they can build those applications without asking for anyone's permission.

5.2. Tragedy of the Commons

But there's one more thing that's really unique about bitcoin, and it's one of the reasons that it continues to survive and continues to win over the centralized, closed networks of the past, and that is that bitcoin is open source, open standard, and open network.

One of the key concepts in economics is the idea of a tragedy of the commons. This is when you have a common resource that can be consumed, without limits, by all those who participate until the resource is depleted and the entire system collapses. It's a form of market failure called "the tragedy of the commons." The most common example of it is the commons, in the old British sense, of a large grassy area. Here you have a field that everyone can graze their cattle on, and if everybody goes and grazes their cattle with reckless abandon, before long, you have a big muddy pit and no cattle. Because everybody overgrazes it, the resource is depleted.

5.3. Festival of the Commons

Bitcoin doesn't suffer from a tragedy of the commons like most financial networks do. I can't innovate on somebody else's network. When Visa innovates, only Visa wins. When MasterCard innovates, only MasterCard wins. If a feature is deployed on SWIFT, I don't get it as a consumer. If Bank of America makes something new and snazzy, they do it competitively and at the exclusion of every other bank that didn't implement that feature.

Bitcoin is a common resource whose use increases the value of that resource, at the exclusion of no one. If a company builds a new feature that can be used on bitcoin under an open-source license, that feature can then be used by everyone in the ecosystem. That means the innovation enriches everyone in the network. If a company invests money in bitcoin, the protocol, they benefit, but so does everybody else. When they play in the bitcoin sphere, they get to benefit from everybody else's investment in that space. So, it returns multiple times. You get this wonderful synergy where each company that invests in this amazing technology makes it better for everybody else. It's not an exclusionary principle; instead of a tragedy of the commons, you have a festival of the commons. A commons that gets better when more companies use it.

"It's not an exclusionary principle; instead of a tragedy of the commons, in bitcoin you have a festival of the commons. A commons that gets better when more companies use it."

5.3.1. Festival of the Commons 2012-2014

Just look at some of the examples. 2014 was supposed to be the worst year in bitcoin. But that's only if you're focused on price, because in 2014 we saw the deployment of two incredible technologies. The first is multisig, which required a tiny change to the core protocol but then allowed an enormous amount of services and products to be built at the edge. The second is hierarchical deterministic wallets, which didn't require any changes to the core and allowed us to have these incredibly complex and rich experiences in the wallet space. The companies that invented and deployed those two features did so in 2012 and we reap the benefits today. An entire ecosystem of new products and services have been built from those two inventions. The value invested by one company two years ago blows up and creates an entire range of products in a new industry two years later.

In 2014, during the worst year of bitcoin, 500 startups received \$500 million in investment, generating tens of thousands of jobs, and none of that innovation has come back yet because they just started. All of the incredible technology advancements we saw in 2014 grew from inventions in 2012. Now, what happens when you throw 500 companies and 10,000 developers at the problem? Give us two years and you will see some pretty amazing things in bitcoin. And that is the advantage of the festival of the commons.

5.4. Accelerating Innovation

While journalists are writing yet another obituary for bitcoin, I see an ecosystem of openness. I see an ecosystem that is generating jobs in an economy that is mostly dead. I see an ecosystem that has some of the smartest people I have ever met creating the most amazing innovations. And the really amazing thing about this is that we all benefit from all of this. We're not really competing against each other. We are participating in the festival of the commons, and as a result we're seeing a rate of innovation that is accelerating. It's already at breakneck speed, and it's accelerating.

Take an open, decentralized ecosystem with a festival of the commons — open source, open standards, open networking — and the intelligence and innovation pushed all the way to the edge so the users have control over what they innovate and how they invest their time and money and spirit into this technology. Put that against a closed system, controlled by a central provider, whose permission you need in order to innovate and who will only innovate at the exclusion and competition of all of the other companies. We will crush them.

People ask me, "Well, what happens if Goldman Sachs builds GoldmanSachsCoin?" I say, let them build it. If it's really open and decentralized, they just proved the whole point of this and we can all go home declaring victory. If it's closed and doesn't allow open innovation, it will become stagnant in just a few months while we continue accelerating ahead with more and more innovation feeding off each other's invention.

You cannot stop this. That's why I'm excited to be in the bitcoin space: a dumb network that puts all of the intelligence and innovation at the edge so that we can innovate without asking anyone's permission, and we can participate in this incredible festival of the commons.

Thank you.

Chapter 6. Infrastructure Inversion

Zurich Bitcoin Meetup; Zurich, Switzerland; March 2016

Video Link: <https://www.youtube.com/watch?v=5ca70mCCf2M>

Today, I'd like to talk about a concept that I like to call *infrastructure inversion*. I'm going to talk about how things change when a new technology must first use the old infrastructure, and how that creates a conflict, pressure that can lead to an infrastructure inversion.

6.1. New Technologies, Riding on Old Infrastructure

Bitcoin is new. Bitcoin is different. When I use the term *bitcoin* here, I'm speaking broadly. What I'm talking about is decentralized network-centric platforms. These platforms can be used for currencies, payments, and other trust applications. The platform could be bitcoin, or something else. For this talk, I'll use the term *bitcoin* to cover that whole category that has now been created. It's new, and we're trying somehow to squeeze it on top of the existing banking system. The result is messy.

Not only is it messy, but it's also an opportunity for those who support the traditional banking system to say, "See, it's not working. It's slow. It doesn't work so well." This isn't new. This is a phenomenon that happens every time you have a new technology that is disruptive, that in the first few years of its adoption it has to be carried by the existing technology that it is disrupting.

"Every time you have a new technology that is disruptive, in the first few years of its adoption it has to be carried by the existing technology that it is disrupting."

Let's take a historical look at how these things play out. When you read about a disruptive technology 20, 30, 40 years in the future, it is all very smooth. It's obvious because hindsight provides clarity. For example, automobiles were a great invention. And of course when automobiles were invented, everyone in the world said, "Yay! We don't need horses anymore." Right? That's not exactly what happened. Instead, they said, "That's crazy. Those noisy disgusting machines that are probably going to kill us all, they'll never work. And why would anyone other than stupid rich people playing with these crazy noisy toys want to use one of these horrible machines when we have perfectly good horses?"

This is what actually happens throughout history when you introduce a disruptive technology. You meet resistance. Resistance is the first reaction. The ones who succeed are the one who continue—even though the rest of society tells them they're crazy—to pursue a crazy idea: automobiles, electrification, the internet, bitcoin. These crazy pioneers, who were made fun of by everyone else in society for their crazy ideas, persisted until everybody could see that what they were doing was correct.

6.1.1. Infrastructure for Horses

Looking at that history, one of the really interesting things to me is that in the beginning, the disruptive technology has to live in a world created for the technology it's replacing. When you first ride your brand new automobile in a city, you are riding on roads used by horses with infrastructure designed and used for horses. There are no light signals. There are no road rules. There are no paved roads.

"You are in horse society and you are the crazy one driving one of these horseless vehicles."

There are a few things about horses that cars don't have. These early cars were forward-wheel drive. So, just two wheels turning. Horses are four-foot-drive vehicles, which gives them a lot of flexibility. They also have balance. You had a road that was designed for horses and it was not paved. Some of them had cobblestone, but the vast majority of roads were not paved. They were also not dry. They were usually covered in mud and horse poo (because that's what horses do). This is the environment that the automobile had to prove itself in. It didn't start out with "Yes, great, we have now invented an automobile. Allow me to demonstrate its capabilities on the Autobahn." Instead, the crazy rich people who were experimenting with this technology were driving their cars on roads with deep ruts, where the horses had been. On roads not designed for automobiles, in mud. And what happened? The cars got stuck because they didn't have balance and four feet.

The critics said, "Ha, we told you this is never going to work. Look at yourselves. You can't even get out of the mud. Also, where are you going to get gasoline? There is only one gasoline station. What happens if you run out of gasoline before you get there? I mean, if your horse gets hungry, you could at least go a few more miles, but if your new crazy car idea runs out of gasoline, that's it, you're stuck. You were already stuck because of the mud, but now you are really stuck because you ran out of gasoline. This is never going to work."

6.1.2. From Horses to Vehicles

Often, new technology must first use the infrastructure of the technology it will eventually replace. In the beginning, automobiles had to use roads designed for horses. Eventually, we started paving roads. Then, something really interesting happened. When you pave roads and make them suitable for vehicles, the old technology (horses) can still use them. If you want to do a nice tour of Zurich on horseback, I am sure the horse would be perfectly comfortable. Horses are very comfortable on asphalt, as are skateboards, Segways, motorcycles, and bicycles — technologies that didn't exist. In fact, in order for those technologies to exist, you first had to build the infrastructure for automobiles.

Flat, paved roads not only allow the automobile to exist, allow the horse to comfortably exist, but they also open the door for new technologies. Now, you have people riding Segways, scooters, skateboards, rollerblades, pushing prams and all of the other things that are moving around on our streets.

That's an infrastructure inversion. You start with the new technology living on the old infrastructure and then, it flips. You build infrastructure and then the old infrastructure rides on top, on the infrastructure designed for the new technology.

"That's an infrastructure inversion. You start with the new technology living on the old infrastructure and then, it flips."

Let's look at more examples.

6.1.3. Infrastructure for Natural Gas

One of the great things about history is that some of the most confident proclamations are often ridiculed for centuries because they are so ridiculous. For example, when electrification was introduced during the World's Fair in Paris, the mayor of Paris at the time said, "Electricity is a fad and as soon as we close the fair and take down the Eiffel Tower, electricity will vanish in history." Wrong on two counts. The Eiffel Tower is still standing and electrification won.

But think about the time when electrification was just beginning: there was no infrastructure. So how exactly do you put electricity into a home? First of all, the only reason to put electricity in the home is because you are one of those crazy rich people. Probably one of the same people that bought an automobile. You are now basically putting lightning in your walls, which is surely a crazy idea that will result in your house burning down. That's what the newspapers wrote. They wrote about every house that burned down and how these crazy people were putting electricity in their homes.

What was the infrastructure at the time? Back then, most of the infrastructure was designed to deliver gas. In fact, gas lighting in major cities was pretty common. There were pipes that could deliver gas primarily to street lights but also for home lights, as well as heating. You couldn't use that infrastructure for electricity. You couldn't use it to distribute electricity to homes.

At first, the only use for electricity was really for factories because that's where you could make the most use of electricity. Prior to electricity, a factory might have a very large gas-driven motor sitting in the corner of the factory. The motor distributed power through a series of belts and pulleys distributed throughout the factory to run all of the other equipment. It was basically a gas turbine.

Electricity allowed you to distribute electricity directly to all of the equipment and use electric motors.

Obviously, factories could benefit from electricity, but why put it in your home? Why would you use electricity since you already had light and heating from gas and it worked fine? And there was no infrastructure. The infrastructure for gas wasn't useful for electricity. If you wanted it, you'd have to build new infrastructure.

Then we see the other aspect of this infrastructure inversion, which is that those invested in the status quo point to your new electricity projects and say, "There is not a large enough distribution network to create customers. And there are not

enough customers to require a distribution network. This is never going to happen." Which is exactly what they said about cars. They said, "There are not enough gasoline stations to fill your cars and there are not enough customers to require gasoline stations. This will never happen."

6.1.4. From Natural Gas to Electricity

Then, electrification starts happening, and people discover that once you put down electricity infrastructure, not only can you use that to do the new electricity capabilities, you can also use it to do the old applications. You can do light and heating and you can do them more effectively, in some cases, with electricity. But now, you can do new things. You can do fans and you can do air conditioning and you can do motors and you can do mixers and you can do hairdryers and, generally speaking, houses don't burn down because of electricity too often.

Again, we see infrastructure inversion. For the first few years, you have to run on the old infrastructure. It's almost impossible. You could theoretically attach a gas generator in your house and feed it with gas and generate electricity locally, but that wasn't very efficient. Then, you build infrastructure for the new technology, and that infrastructure enables the old technology quite comfortably—lighting, heating, or horses, in the case of roads. But it also opens the door for new applications that you couldn't do before. And the world changes.

"Changing the infrastructure opens the door for new applications that you couldn't do before. And the world changes."

6.1.5. Infrastructure for Human Voices

My third example is a bit more technical. This is where you'll see the audience separate into those who are over 35 and those who are under 35. Tell me if you can recognize this sound.

Andreas replicates the sound of a dial-up modem

People under 35 are looking at me like I am crazy, and the people over 35 are saying, "That's a modem. I used to have one of those! That's how we connected to the internet." Forgive me as we go into ancient history. A modem is a modulator-demodulator. It's a device that speaks data over a telephone line. Here is the thing: if you think about it, the telephone line is like a dirt road and you're trying to drive a car over it.

A telephone line is a system designed to carry human voice. When I was a teenager, telephone lines were still analog and we had pulse dialing systems. We used to sometimes try to play music to our friends over the phone line. If you'd ever tried this, you would have discovered it didn't really work. The reason it didn't work is because the frequencies that a telephone line allows are very narrow.

You see, the telephone network is designed to do one thing and only one thing. It's highly specialized, just like the gas network that delivers gas to houses is only designed to deliver gas. Not water or electricity or oil. Just gas, and it's specialized. The telephone system was designed to deliver just voice, and human voice is very specific. Our main frequency is 1 kilohertz; we stay close to that range, sometimes going a bit above and a bit below. There are a few people who can go quite a bit beyond a common range. Teenagers can go to frequencies that I can't even hear anymore. But because of the specialized use of voice and because of the difficulties of transmitting voices, especially over great distances, engineers narrowed the acceptable range. If you allow a full range, you get voice but you also get static noises, electrical interference at very high frequencies. You also get humming noises, electrical interference from motors at very low frequencies. What happens if your phone line has static and humming noises? You add a filter that chops out the lows and another filter that chops out the highs. Now, the connection is cleaner but the human voice starts sounding weirder and weirder because it's being compressed.

This compressed road is a very difficult road to ride data over because when you're transmitting data, you need to get a lot of information into a very narrow

frequency band. The whistling sound that you hear with the modem is actually two modems trying to test the available frequency range on this specific connection. All of those noises are the modems saying, in different frequencies, "Can you hear me now?" and the other saying, "I heard you. Can you hear me?" back and forth until the available range is established.

This is an insane way to do data transmission. You've basically got two devices that are singing to each other over a very narrow channel, trying to somehow squeeze as much data as possible through a narrow little straw. Then, we upgraded them and they got better and better at doing this.

The phone companies hated it: "That's not what we designed the networks for. This is a pristine, state-of-the-art voice-communicating network. What the hell are you people doing?" In fact, in the country where I grew up—in Athens, Greece—if you tried to make a long-distance call with the modem, what you would hear is the beginning of a modem connection and then an abrupt click. What? What just happened? They cut off the lines if they detected a modem. Why? Because it was competing against the phone company. Kind of like banks shutting down accounts of bitcoin companies. Or basically, exactly the same.

What did they say at the time? They said, "We could deploy data connections—fiber, coaxial cables, direct data connections at high bandwidths. But first of all, no one needs high bandwidth because what are they going to do? Transmit voice? We already have a voice network. It's fantastic. We don't need these new things. Secondly, you don't have enough users to deploy coax. And you don't have enough coax to build a user base. This is never going to happen." The same exact idea.

6.1.6. From Voice to Data

Then, we had one of most spectacular examples of infrastructure inversion that I have ever seen and that I recall from history. When, first, the internet was not wanted and carried over phone lines reluctantly. Then, the internet was carried over phone lines by phone companies becoming internet service providers. Then, gradually their backbones become data-oriented. Then, their entire network becomes digital. Then, their entire network starts running over the internet. Then, they start running all of their phone lines on top of the internet. Today, every single phone call you do anywhere in the world is carried over the internet, with a few exceptions at the edges in some developing countries. A complete infrastructure inversion.

"Today, every single phone call you do anywhere in the world is carried over the internet, with a few exceptions at the edges in some developing countries. A complete infrastructure inversion."

It turns out, it's very difficult to push data through a narrow phone line designed for voice, but if you flip the equation, putting voice over a data connection is trivially easy. What's the difference? One is extremely specialized. It had already chosen the application for you. The application is voice; data is the exception that you're trying to squeeze through. The other one is very generic. Data means anything, and voice is just one of the applications carried comfortably.

I think the ultimate irony for the phone companies was that special thing called "comfort noise generation." If you're a phone engineer, you know what I'm talking about. This is the most ironic thing ever. After years and years of people my age being used to their phone line having static all the time, when we started having cellular telephony and digital phone lines that were perfect, they had no noise. The moment the other person stopped talking, what you would have was complete silence. So, you were like "Oh, okay, I guess they hung up."

They didn't hang up. They were still there. There was just none of the static. Then, the phone companies invented the most brilliant technology ever, which is comfort noise generation. This is a device that sits on your end of the phone and it looks to see if the connection is still open, and if it is, it whispers static into your ear just to make you feel comfortable that the other person is still there. It actually generates high-frequency noise on purpose, artificially on your end—noise that isn't in the system, just so that you don't think the other person has hung up.

The very same companies that said, "We will never be able to do quality voice over the internet. We don't want the internet on our phone lines," are now

injecting noise in order to simulate the terrible performance of the previous network because we're now delivering CD-quality or better sound across continents. Complete infrastructure inversion.

6.2. From Banking to Bitcoin

Now, we have bitcoin. We have a decentralized trust platform that can do settlement of transactions on a global basis without intermediaries. But we're still living in the old system. Today, we have to use exchanges tied to traditional bank accounts, or use IBAN transfers, or credit cards. Today, we're riding the automobile along the muddy roads of banking. The bitcoin supercar, the Formula One of finance, is riding along on the muddy roads of 1970s mainframe-based banking, and it's a bumpy road.

"The bitcoin supercar, the Formula One of finance, is riding along on the muddy roads of 1970s mainframe-based banking, and it's a bumpy road."

The banks point at this and say, "It's not working. Look, you have to do all of the regulation that we have to do. You have to do all of the identity that we have to do. You have to slow everything down to the speed of traditional banking. This is never going to work. Not only that, but you don't have enough users to build infrastructure, and you don't have enough infrastructure to attract new users. So, this is clearly never going to work."

But what we *do* have, just like with electricity and the automobile and the internet, is a new technology that has within it the promise of a thousand other applications they haven't even imagined.

I predict, over the next 15 to 20 years, we'll see a great infrastructure inversion happen in finance. First, the banks will resist. Then, the banks will adopt. The banks will run their systems alongside blockchain and bitcoin systems, and finally they will run all of traditional banking as an application on top of a decentralized trusted ledger. Because, while it is very hard to do a decentralized trusted ledger that's connected to all of these legacy banking systems, simulating legacy banking on top of a decentralized ledger, on top of bitcoin, an open global blockchain, is trivial. All you have to do is take all of its capabilities and slow them down. For example, I can create an application that takes your bitcoin transaction and makes it clear in three to five business days for a cost of 5 dollars. I have implemented traditional banking. It's kind of like comfort noise generation.

"Over the next 15 to 20 years, we'll see a great infrastructure inversion happen in finance."

For those of us so accustomed to the banking of a previous generation who say, "I don't like all of this fast finance. It makes me uncomfortable. I want to sit at my kitchen table every Sunday and balance my checkbook and make sure none

of my checks bounced. I don't like all of this electronic instantaneous global transfer. It scares me," we can slow it down.

This infrastructure inversion will allow us to comfortably run traditional banking applications on top of a distributed global ledger — an open blockchain like bitcoin, *the* open blockchain, probably bitcoin's open blockchain and simultaneously open the door for other applications, for applications we've never seen before. These new applications will look different from traditional banking. As different as a Segway or skateboard looks to those committed to traditional horse-carriages. As different as moving to electricity in an era of gas lighting in traditional Victorian homes. As alien as comfort noise on high quality data voice communication over the internet that is capable of so much more.

Enabling the future on your legacy system is very difficult. While you're trying to do that, everyone is pointing at the future and saying, "Look. It doesn't work." Once you flip the infrastructure, simulating the past on the network of the future becomes extremely easy.

"Once you flip the infrastructure, simulating the past on the network of the future becomes extremely easy."

What we're part of now is the very early stages as we look at the future of money, and the first stages of the greatest infrastructure inversion the world has ever seen.

Thank you.

Chapter 7. Currency as a Language

Bitcoin Expo 2014 - Keynote; Toronto, Ontario, Canada; April 2014

Video Link: <https://www.youtube.com/watch?v=jw28y81s7Wo>

This is going to be a bit more of a philosophical talk about the future of cryptocurrencies and what I've learned here at this event. This event is called the Bitcoin Expo 2014. It might have been called the Bitcoin and Ethereum Expo 2014. I don't know if you noticed, but Ethereum had a pretty big presence here. An interesting question comes up, actually quite a few people have asked me: "Does Ethereum threaten the future of bitcoin? Does it steal some of its thunder?" Those are questions I've heard several times, and I've heard people refer to that issue in trying to understand altcoins - wondering whether altcoins essentially threaten the dominance of bitcoin, if they make bitcoin weaker, if they distribute the value of the network too broadly.

7.1. Born into Currency

I've been thinking about this question for quite a while. I think, fundamentally, it's a question that evokes the old paradigm of currencies. We've all grown up in a world where currencies are forced upon us in a monopolistic fashion, where currencies are defined strictly by the geographies in which they occur, and where the choice of currency is not yours. It is an accident of birth, just like many other things in our lives. As an accident of birth, I was born into an upper-middle-class family in Greece, fully loaded with a lottery of privilege in my life. I also acquired the drachma. I didn't choose the drachma any more than I chose to be a white male, any more than I chose to be born into a family of educated people. Those things simply happened to me.

"Currency is an artifact of the nation-state. It imposes upon us a certain constraint. We don't choose our currency; it chooses us."

Currency, as we understand it, is an artifact of the nation-state. It imposes upon us certain constraints. We don't choose our currency; it chooses us. We are forced to use that currency in all of our interactions. We don't have a choice — until 2008, that is. We now live in a slightly different world, but a lot of the old paradigm persists in our thinking.

In a world where your currency is a monopolistic nation-state artifact that is constrained by geography, it's a zero-sum game. The currency is the flag, is the nation-state. It is the expression of the economic value of your state. It defines your interactions in a world of geopolitics, in a global struggle for domination among nations. It's not up to individual choice. It has nothing to do with the individual, except for that one individual whose face is on the currency — up until recently here in Canada, some old white lady named Elizabeth.

7.2. Currency as a Means of Expression

Now, we live in a new world, a world in which currency is a choice, and not just a choice in terms of use. It's not just a matter of being able to choose which currency we use as individuals. It's also a means of expression. Any of us can now create a currency using a simple web form.

"Now, we live in a new world, a world in which currency is a choice, and not just a choice in terms of use... It's also a means of expression."

As I thought about the evolution of alt-currencies, as they're called, I realized I was asking the wrong questions. How many currencies will there be? How many altcoins will there be? How will altcoins compete in a world of cryptocurrencies as we move into the future? Will there be hundreds of altcoins? If there are hundreds of altcoins, what does that mean for the value of each of the altcoins? How do they compete? That was the wrong way of thinking about it. I saw currency as a zero-sum game, just like it had been imposed on my worldview from the nation-states that created currency. Then, I started thinking of currency as an application. And then, I started thinking of currency as a means of expression.

You see, money, at the very root of it, is a language. It's a language we use to express value to each other. When I give you a dollar bill, I am saying that I want to hand you the equivalent value. I'm communicating my desire to exchange value with you, because I appreciate something you can do or something you can give to me. I'm using money as a token of language.

"Money, at the very root of it, is a language. It's a language that we use to express value to each other. When I give you a dollar bill, I'm saying that I want to hand you the equivalent value. I'm communicating my desire to exchange value with you."

7.2.1. Inventing Currency on the Playground

This happens in human societies whether you have formal currencies or not. If you don't have a currency with a stamped face on it, you invent it. One of the things that really captivated me was understanding that if you have a primary-school environment and you watch children in their natural habitat (a very unnatural habitat in most schools), young children don't have currency, and they don't understand currency. But they invent currency. They start trading. Rubber bands, Pokemon cards, Tamagotchi, tokens of affection, tokens of popularity. Humans create currency as a means of expressing their desires, of expressing their individuality. I thought, What happens when a five-year-old in a primary school can use a website to create Joeycoin to compete against Mariacoin in a game of popularity within their school?

Then it dawned on me: To ask the question, "How many currencies will exist?" is equivalent to asking the question, "How many bloggers will there be on the internet?" The answer is simple: all of us.

Currency is now a means of expression. But if everyone can create a currency, how does it derive value and what does it mean? What is the difference between currency as an expression of popularity, as an expression of desire, as a meme, a fad, a brand? Down there right now, *Andreas points outside of auditorium*, a Canadian teen idol contest is running. One of those contestants, Amir, has a big fan group. Maybe he wants to create AmirCoin so that his fans can express their desire to watch more of his dancing. Why not? People have talked about me doing AndreasCoin. I think it's a bit silly. But, why not? I think at some point we're going to see things like that happen.

We're not going to have hundreds of altcoins. We're not going to have thousands of altcoins. We're going to have hundreds of thousands, and then millions of altcoins. Then, there will be thousands of altcoins being created every day to organize local communities to express fads, to create popularity contests, to codify the latest internet meme.

"We're not going to have hundreds of altcoins. We're not going to have thousands of altcoins. We're going to have hundreds of thousands, and then millions of alt-coins."

7.3. Authority by Production

With so many altcoins, how do you tell which ones have value and which ones don't? In order to try to answer these types of questions, I often reflect on the emergence of the first decentralized system in my lifetime, the internet. What it did for understanding information, information scarcity, opinion, and authority of opinion. What it did to us as a society as the internet emerged into our global scene.

There used to be a time when if you wanted to read authoritative opinion, you bought a piece of paper from an organization that had a printing press that was three stories high and four football fields long and had a really great name, like *The New York Times*. That organization could buy ink by the barrel, and through that ownership of this enormous manufacturing facility, they had the weight of authority. We imbued authority into these institutions, and we used that authority to decide which opinions mattered and which opinions didn't. We used them as gatekeepers of authority to give us guidance in understanding opinion.

Then, the internet destroyed all of that, because suddenly *anyone* could print, *anyone* could publish.

7.4. Authority by Merit

In the early days, people asked, "How will we know which opinions matter if anyone can have an opinion?" The world will come to an end, they thought. But a funny thing happened. We shifted from a world in which authority and opinion came from the issuer, from the authority of the publisher by proxy, into a world where we had to look at opinion on its own merits, on the content of that opinion. We arrived at a world where *The New York Times* prints bullshit that sends an entire nation into war, and an Egyptian blogger on the front lines of a revolution prints the truth that nobody wants to hear. Suddenly, the world is upside down. Authority is no longer the person who owns the printing press. Now the person who has the content is what matters — we just did this to currency.

"Authority is no longer the person who owns the printing press. Now the person who has the content is what matters — We just did this to currency."

7.5. Valuing Currencies by Use

Now, the authority is not derived from the sovereignty of the issuer, from the printing press of a nation-state that can declare through monopoly and use of force that this is the currency you will use. Now, we can choose currency, and a five-year-old can create currency. Maybe the currency that the five-year-old created has monetary value, maybe it doesn't. Most likely, it doesn't. But some will. We need to get used to a world where we have to judge currency not by who issued it, but by who uses it. Or rather, by how many people use it and what they use it for.

"We need to get used to a world where we have to judge currency not by who issued it, but by who uses it. Or rather, by how many people use it and what they use it for."

Let's imagine a world in which a currency is being used in a widespread fashion, and no one remembers who created the currency or why. They only know that within their local community, it has purchasing power. As a little fanciful thought: Imagine a decade from now, in a rural village detached from developed-nations, villagers exchanging two currencies. One has a Shiba Inu, a Japanese breed of dog, on the front and is pronounced *Dogecoin*. I'm not quite sure how to pronounce it and it doesn't really matter, but you can buy half a dozen eggs with it. The other villagers are trading another currency that has an old white lady named Elizabeth on it. They have no idea who Elizabeth is. They don't know why she got her picture on the coin. Maybe she wrote a nice song. Maybe she won Canadian *Teen Idol*. Nobody remembers anymore, but you can buy six eggs with it.

To those people, it doesn't matter who issued the currency; what matters is whether it has purchasing power or not. The currency is now evaluated purely on its monetary basis, because of adoption, because of use. There is one fundamental difference between those two currencies. One has a predictable, stable, algorithmic monetary supply. The other has an old white lady named Elizabeth on it. So, in fact, one of them has some real intrinsic value because it has removed some of the uncertainty of the monetary system from it. The other one doesn't really.

We need to get ready to live in a world where multiple currencies will coexist.

7.5.1. Multiple Currencies Coexist

Currency as a means of expression, currency as a tool of language, is no longer up to the issuer. It is up to us as individuals making a choice to use that currency, and we give it value through our use. We give it value through adoption. We will be surprised by some of the currencies that will emerge from a fad, a joke, perhaps even a sick joke, and will explode into viral consciousness on the internet and then become real monetary powers in use across a broad population.

How do we operate in that kind of world? What does it mean to have competition between currencies if there are millions? What if digital scarcity really applies, but only on a local basis and only in the context of each of these currencies? What if scarcity is not derived from the issuer but is derived in terms of adoption and in terms of the token itself?

"Currency as a means of expression, currency as a tool of language, is no longer up to the issuer. It is up to us as individuals making a choice to use that currency, and we give it value through our use."

We're going to have currencies for different uses. Already, you have bitcoin that provides a very specific monetary policy. You have Ethereum that can provide a contract platform. There's Namecoin for distributed naming conventions. There are many others, and there will be many others that will solve other problems: protein folding, the search for extraterrestrial life. Maybe we'll have currencies that are better for microtransactions and micropayments with very fast resolution. Maybe we'll have currencies that are better for larger transactions, like real estate. Who knows. If you think of currency as an application, then you realize that it doesn't really matter.

On the internet, email was the granddaddy of them all. Or the grandma of them all. Email, like bitcoin, was the killer app that allowed us all to see the power of decentralized communications and adopt this new platform. It was enough to create utility to spread this network all around the world, but it was only the first app. Then, instant messaging, forums, bulletin boards, Facebook, Twitter. Do you worry that Twitter will destroy email? Do you worry that Facebook will destroy instant messaging? Do you worry that the value of email is eroded somehow by the existence of Twitter? We don't worry about these things because we understand that each one serves a different purpose. Some allow us to express a modality of instantaneous, real-time communication. Some allow us to have asymmetric communication, where using Twitter I can address an audience of thousands and receive real-time feedback without having to have a bi-directional, synchronous communication. Some, like email, allow us to have

more long-term, asynchronous communication between people.

What we do is we build interfaces, we build abstractions, we build unifying tools that allow us to use all of these modalities from a single interface and fluidly move from one to the other. So, we can start transmitting a short text message to someone, get into a conversation, convert that to an audio conversation, decide that we want to show them our dog, turn on the video camera, convert it into a video conference, and when we're finished with the conversation, follow up with an email to summarize what we've agreed on. Now we've gone through five different modalities of communication in a single unified interface.

"What we do is we build interfaces, we build abstractions, we build unifying tools that allow us to use all of these modalities from a single interface and fluidly move from one to the other."

7.5.2. Currency as an App

I think that's what's going to happen with currency. We're going to start treating currency as an application, and in order to do that we're going to need interfaces that allow us a unified currency experience, that allow us to have a single wallet with perhaps 150 different currencies in it. Because of inventions like sidechains, decentralized exchanges, fluid liquid systems and the complete absence of monopoly, of lock-in, of hostage situations around the currency, we will be able to instantaneously and at very low cost convert from bitcoin to Namecoin to Dogecoin to Ethereum. If we can do that, then it doesn't matter because we won't do that; our unified wallet interface will do that, by trying to see what we're trying to achieve with our currency. If I'm buying a house, it might express my transactional will in the modality of bitcoin because that is the most suitable currency. When I try to name the domain for that house, it will convert some to Namecoin. The contract itself will be paid in ether. When I tip the bartender for the cup of coffee they gave me when I got up that morning, I'll tip them in Doge. My interface will hide all of these differences.

"We're going to start treating currency as an application, and in order to do that we're going to need interfaces that allow us a unified currency experience, that allow us to have a single wallet with perhaps 150 different currencies in it."

I can see a world in which we can smoothly move between currencies in a multimodal way. There's one other thing that comes out of this, which is the very real possibility that we will abstract value in exchange rate from the actual currency. If we have a multimodal communication system, we no longer need to look at the individual values and exchange rates of all of these commodities, assets, currencies, call them whatever you want.

7.5.3. Index Currency

There's a very real possibility we're going to have an index currency: a currency that is not in itself tradable, that has no intrinsic use as a transactional commodity, but instead is only used to express the purchasing power vis-a-vis the various coins in our wallets. I may have a thousand unified currency units. You can't buy unified currency units. You can buy bitcoin and then you can tell me how many unified currency units that is. I price everything in unified currency units, and then I pay in Dogecoin or Namecoin or bitcoin or Ether, depending on how I want to use it.

"I can see a world in which we can smoothly move between currencies in a multimodal way."

We already do this in financial markets. In fact, you can trade S&P 500. You're not buying a single company; what you're buying into is the aggregation of all of the different things that are in the stock market as an expression of the total value of the market. You can then use that meta-instrument in order to price transactions. For example, the London Interbank Offered Rate is used as a meta-interest rate to contractually tie things to a global set of interest rates. You don't need to say, "I will buy this at whatever the Bundesbank says." You say, "I'll buy this at LIBOR plus 2," and then you have a stable point of reference for transactions.

I expect we're going to see much of the same with currency. We're probably going to see meta-currencies whose only purpose is to aggregate the value in all of our wallets for all of our currencies, and allow us to understand value as an abstraction that exists independently of the currencies in which it's expressed.

7.6. Choosing Currencies and Communities

So, that's a slightly philosophical perspective. That's why I think it doesn't matter: Ether is not competing with bitcoin; bitcoin is not competing with Litecoin. They are all means to express the transactional modality we want to use at any point in time to achieve our goals. With this comes a very important and powerful tool. In the choices we make with these currencies, we are also choosing to align ourselves with a community.

"Adoption is not simply the act of using the currency; it's also attaching oneself to a community that has also chosen to adopt that currency."

Adoption is not simply the act of using the currency; it's also attaching oneself to a community that has also chosen to adopt that currency. When I choose to adopt bitcoin, I am a believer in a monetary policy of 21 million total coins as a stable source of value. If I choose to adopt Freicoin, I am a believer in an inflationary-basis, demurrage coin that has a negative interest rate, that enforces consumption and discourages hoarding. I am choosing my politics through my currency, and through that choice I am associating myself with a global community that has made the same choice as me, and that is expressing that choice through currency. Just like when I choose an application on the internet to communicate with, I'm also aligning myself with a corresponding community. I don't use Twitter just because it's a convenient communication mechanism. I use Twitter because I also agree with many of the concepts and philosophies of the community of other people who choose to use Twitter.

"We have entered the realm of meta-politics, of politics by algorithm, of the ability for global communities to form around a common consensus of politics through the choice of currency."

With currency, that choice is a much more powerful political choice. We have entered the realm of meta-politics, of politics by algorithm, of the ability for global communities to form around a common consensus of politics through the choice of currency. You want inflation? Use an inflationary currency. You're a goldbug? Use a deflationary currency. You want a currency that creates a guaranteed minimum income for the poor? Use a currency that expresses those politics. You want a currency that puts aside tokens for carbon sequestration? Use a currency that expresses your green politics. We're going to start seeing communities, politics, and currencies converge and allow us to make these choices. Just like I can support Joeycoin in order to say that Joey is in fact the coolest kid among the five-year-olds, I can support Greencoin because I care about global warming. Or not. I can support Meatcoin if I really really like red

meat. Whatever. WorldWideWrestlingCoin, no problem. There'll be one of those, too.

Really all of these things are forms of expression, and that comes back to the original point: that currency, in the end, is really a form of language. It's a language by which we communicate our expectations and desires of value, and now that we can do it on such a massive scale, now that everyone can create currency, our choices will really matter. We're past the zero-sum game. This isn't about nation-states anymore. This isn't about who adopts bitcoin first or who adopts cryptocurrencies first, because the internet is adopting cryptocurrencies, and the internet is the world's largest economy. It is the first transnational economy, and it needs a transnational currency.

"This isn't about nation-states anymore. The internet is the world's largest economy. It is the first transnational economy, and it needs a transnational currency."

7.7. Currency Creates Sovereignty

To summarize, we've inverted the very basic and most fundamental equation of currency. For millenia, until the year 2008, sovereignty defined currency. Sovereignty was the basis upon which currency could be created, and that currency allowed that sovereignty to be expressed. The monopolistic control of currency is the basis of sovereignty. Now, the internet has a currency. The internet is going to use that currency to create sovereignty.

"After 2008, currency creates sovereignty."

After 2008, currency creates sovereignty. The internet has its own currency, which means that the internet has purchasing power. Which means the internet has economic freedom. Which means the internet can exert that economic freedom in a post-nationalist way, in a way that ignores borders and makes the nation-state not obsolete, but simply less relevant. When an Egyptian blogger can not only blog about the revolution but also fund that revolution in bitcoin, and they can connect with people from all around the world who share their ideas for self-determination and freedom, they are expressing their own sovereignty as an individual, and they are expressing the sovereignty of their community through the use of that currency.

This is the world we now live in a world in which currencies can coexist, and where currency and its user adoption create sovereignty.

Thank you.

Chapter 8. Bitcoin Design Principles

This talk was delivered in June 2015, at the Harvard Innovation Lab in Boston, Massachusetts, as part of an IDEO Lab design workshop. During this 2 day workshop, students competed to create prototype applications based on bitcoin and blockchains.

Video Link: <https://www.youtube.com/watch?v=Ur037LYsb8M>

Good morning, everyone. Wow, what a difficult task you have. At a very basic level, you have to try to understand *what is bitcoin*. I can answer that question in four words. Bitcoin is digital money. But that doesn't really capture it. It's more like the internet of money. But really it's a consensus decentralized network based on blockchain technology and a proof-of-work algorithm that allows a digital token to act as a reward system for a game-theoretical competition between decentralized miners who validate—and "Oh my..." it immediately goes off the cliff.

Even after a couple of years of exploring "What is bitcoin?" you'll find you're still learning, you're still trying to understand what it is. Part of the reason for that is because bitcoin is a really new technology, it's a really disruptive technology, but it also is an abstraction on a technology that is really old. That technology is money. Money is a tool, it's a technology. It actually shares commonalities with linguistic structures, because we use it almost like a language to communicate value among ourselves in a society.

8.1. History of Money

Who wants to tell me here how old money is? *Audience member*: "5,000?" Okay, that's a good guess. A bit older. Try again. The problem with trying to understand the history of money is that money is older than history. We can go and look at the writing about money. Money is older than writing. That may confuse you a bit. You're like, "Money's older than writing? That can't be." In fact, if you look at the first forms of writing that we can find, they are spreadsheets. They are accounting ledgers. The first thing scratched onto tablets created with twigs and things like that are accounting ledgers. They represent how many amphorae of oil were given to the pharaoh. If you go even further back, we find ancient forms of money among the ruins of ancient civilizations: beads, feathers, shells, giant stones. Money has taken many forms, but it exists and has existed almost as long as language. This is a truly ancient technology. So, it's not 5,000 years. It's probably close to 500,000 years old.

8.1.1. Primates and Money

In fact, we see money emerge within other species. Highly intelligent species like primates, certain types of birds like crows, even marine mammals like dolphins have forms of tokens that they use to express value to each other. Or they can very quickly learn the mechanics of money. You can teach primates that if you turn in this pebble, you get a banana. And then watch, within a very short period of time, how that not only becomes a part of the primate culture but gets passed down to the next generation, and they start inventing economic activities. Not nice economic activities. They invent strong-armed robbery: beat up the other monkey and take its pebbles, so you can get bananas. They invent sexual favors for pebbles, so you can get bananas. They invent some of the earliest economic activities.

"Highly intelligent species like primates, certain types of birds like crows, even marine mammals like dolphins have forms of tokens that they use to express value to each other."

Money is ancient, it's an absolutely ancient technology, and none of us really understands it. If you want a demonstration of that fact, sit down and have a conversation with a four-year-old and try to explain money. You'll find out very quickly that the four-year-old has very good questions that you can't answer. You can watch parents go through this, it's hilarious:

"Mommy, where does money come from?" "The banks make it." "How do they make it?" "Well, they print it." "Why can't we have more, then." "Go clean your room."

You're about four questions from "Go clean your room" in a money conversation because adults don't really understand money. Even though it is a cultural artifact that has existed in our species for hundreds of thousands of years, we don't understand how it works.

8.2. Characteristics of Money

We've gone through several technological iterations of money. We started with very basic forms of money. These basic forms had certain unique characteristics that made them good as money. What makes good money? Something that is rare. Shells, feathers. You can use shells as money, unless you live on a beach; if you live on a beach, you can't use shells as money. You can transport the value easily. So, it has to be portable. With few exceptions, most forms of money are highly portable. If the amount of money you need to go to buy a cow is heavier than the cow, that's not very good money. Which is why we don't often see, for example, gold being used for large transactions. It's too heavy. Other characteristics of money . . . It has to be difficult to forge; it has to be difficult to create more of it. You should be able to detect at a glance or relatively easily that it is real. It should be fungible. If I'm using shells, then this shell or that shell are both the same money. If I give you a dollar, it doesn't matter which dollar I gave you; it's fungible. Every dollar can substitute for every other dollar.

"Money itself is an abstraction. If it's not an abstraction, then it's not money—it's barter."

These are the technologies, and gradually over time we've created abstractions. Money itself is an abstraction. If it's not an abstraction, then it's not money—it's barter. If I give you bananas for your goat, that's not money. Bananas are not money because you eat them. You don't use them to do further exchanges. Therefore, that's barter. You're exchanging one commodity for another. If it's abstract—if it doesn't have any practical use in itself—then as an abstraction of money it represents something else, some shared value.

Which leads to the one inescapable conclusion about money: Money is a shared cultural hallucination. It's a shared delusion. We walk around and associate with other people on the basis of germ-ridden pieces of cotton printed with green ink. If you were to observe that as an alien anthropologist that landed on Earth, you'd think it was very very weird. That just by exchanging these pieces of cotton, you could create social relationships, transactions, and trade—you could feed yourself, shelter yourself, etc., etc. It doesn't make much sense but it's based on a shared hallucination. It's based on the assumption that if you give me a dollar today, someone else will accept that dollar in exchange for something of value tomorrow. If I still believe that is the case, then it has value. Value comes from the assumption that I can use it again.

"Money is a shared cultural hallucination."

8.2.1. Just Another Abstraction of Money

Bitcoin is just the latest iteration of abstraction. We've done abstraction before but every time we do abstraction of money, society freaks out because this new thing can't possibly be real money. Go back and look at what happened with the introduction of coins stamped onto nonprecious metal, and then eventually paper notes. When paper notes were first circulated, no one believed that they had value. The shared hallucination had not taken hold yet. It was very difficult to persuade people to exchange real gold coins or silver coins for pieces of paper that said that they had gold in a vault. Then, take it a step further, and disappear the gold from the vault and say, "Turns out, it's just the paper."

"...every time we do abstraction of money, society freaks out because this new thing can't possibly be real money."

You ask people about bitcoin, and one of the first things I hear from most people is that it's not real money because it's not backed by gold like the US dollar—which I find astonishing. The dollar hasn't been backed by gold since 1936. Yet, most people think that somewhere in the vault, possibly at Fort Knox or some other movie location, there are bars of gold that correspond ingot to ingot to the pieces of paper that you have in your pocket. They don't. There's no such thing. Why is bitcoin money? Because other people think it's money. You can write a dozen Ph.D. dissertations explaining exactly why bitcoin is not money . . . and I have lived on it for two years. Therefore, it doesn't matter what your dissertation says. To me, it is money, *because* I have lived on it for two years. So have thousands of other people. Therefore, to me, it is very much real money.

8.3. Bitcoin and Design

You've been tasked with creating designs and concepts around the oldest technology in the world that very few people really understand. Its latest, most abstract expression, that is brand new, is completely disjointed from previous expressions of money and is extremely complex as a technology. That is a really difficult task. When faced with that task, your go-to technique is the use of metaphor. Design metaphors are extremely powerful tools. They allow us to create expectations. Metaphors are tools by which we create expectations. When you have a desktop computer and it has a desktop, you assume that something will happen when you drag something across the desktop. Because you've actually used a real desk, that assumption will inform your expectations. You expect it to behave like the object that it's pretending to be. That's a design metaphor. Design metaphors are extremely powerful, but they're also extremely dangerous when misapplied.

"Design metaphors are extremely powerful, but they're also extremely dangerous when misapplied. In bitcoin, every single term and design metaphor is wrong and broken."

8.3.1. Wallets aren't wallets

In bitcoin, every single term and design metaphor is wrong and broken. Let's go through the list. You've probably struggled with this as you've engaged with this technology of bitcoin and looked at all of the terminology. First of all, a "wallet." What is a wallet? A wallet is something that stores money. Not in bitcoin it isn't. The money isn't in the wallet; the money is on the network. The wallet contains keys. So, it's not a wallet; it's a keychain. How can you tell it's not a wallet? Can you copy a wallet? No. But you can copy a key. A keychain is a far better metaphor. If I have a keychain—imagine a big ring of keys like a janitor or a custodian—I have a bunch of keys, and I can go into a shop and have all of those keys duplicated and create a second keychain. Both of those keychains will work interchangeably in all of the locks that the original keychain worked. That's how a keychain works. If you understand what a keychain does, then you will understand how a bitcoin wallet works. You can copy it, you can make copies of the keys. If you give someone a copy of the key, they can open the door. They don't need your permission anymore to open the door.

So, a "wallet" is not a wallet; it's a keychain. That's a terrible metaphor. You have expectations of what a wallet will do. It will contain things. These contents will be discrete and enumerated. None of that exists in bitcoin.

8.3.2. No Coins in Bitcoin

Let's get down to basics: "Bit - coin." *Coin*. What a terrible word. What a terrible brand. *Coin*. Take the most abstract form of money we have ever created, that is based on a completely decentralized network that has no coins, and then name it "bitcoin." Just to confuse everyone. A coin, which is two generations of technology back and a far less abstract, much more tangible, physical representation of money. You took the most abstract representation of money and named it after the most tangible representation of money. Only an engineer could come up with that brand.

Here's a little secret: There are no coins in bitcoin. When miners mine, they don't create coins; they create ledger entries. Those ledger entries do not enumerate coins. They have outputs—transaction outputs—which are chunks of value that are infinitely divisible and recombining. Coins don't do that. You can't track a coin in bitcoin because there are no coins.

So, you've got a "wallet" that doesn't contain "coins"—because the coins are actually on the network and they're not coins, they're outputs—and what you're really holding is a keychain. Transactions are not from a sender to a recipient. Addresses don't have balance in bitcoin. There's no such thing as a balance of an address. An address controls outputs, and if you trawl through the blockchain and add up all of the outputs, you can figure out some notional balance. Whether that's actually spendable or not, how much it is, is actually quite difficult to determine. There is no "balance." You have no "account" in bitcoin.

All of the terms are broken. The problem is, from a design perspective, instead of the metaphor informing our expectations, it is misinforming our expectations. It is creating the grounds for massive misunderstanding, because we think it's going to do something in a certain way, and it ends up doing something completely different, something unexpected. Kind of like the Windows desktop. I don't know if you've ever compared a Mac and a Windows desktop. To me Windows desktops have no consistency. The metaphor is completely broken. You expect it to do one thing, it does something completely different and confuses. The essence of good design is picking the metaphor that informs expectations.

"The essence of good design is picking the metaphor that informs expectations."

8.3.3. Skeuomorphic Design

Here's the next big problem with metaphors and design. There's a certain concept called *skeuomorphic design*. The word *skeuomorphic* means "a shadow of its former self." It's form as a shadow. What it means is when you create elements in design that give you references or hints of some previous form. For example, a classic example, in the first iteration of iPads, the iOS software had a lot of skeuomorphic design. If you opened your contact database, it was bound in leather. That leather had stitching. That stitching didn't do anything. It was just a design element which had no functional purpose, whose intent was to put you into a familiar set of mind so that you could understand the metaphor. When you're playing a card game on your computer and it has fake felt under the cards, that's because it's trying to draw out the metaphor of a casino by introducing this design element. Skeuomorphic design is extremely powerful. It's also extremely dangerous. If you don't use it correctly, again, it creates different expectations as to what is going to happen next.

In bitcoin, we have a lot of skeuomorphic design. My favorite and most hated form of skeuomorphic design is the picture you will see in every single article written about bitcoin: a pile of gold coins with a letter B on them, usually the Casascius coin designed by Mike Caldwell, but possibly some other rendering of that. Taking the worst design metaphor of bitcoin, the word "coin," and then instantiating it in a beautiful rendering that makes it even more physical looking, in a skeuomorphic design that completely misleads everyone. People are actually going out on eBay and they're buying what they think is "bitcoin." They're buying gold-plated, physical coins that have nothing to do with the blockchain but have the letter B stamped on them. "Look, I've joined the revolution of digital money" they say, but these tangible replicas rarely have any value in bitcoin. This is the result. Then, people write articles, and they look at the picture and they think, "So that's what a bitcoin looks like." That's not what a bitcoin looks like, because if you remember, I may have mentioned, there are no coins. This is the danger.

8.4. Designing for Innovation

It's a really difficult task to design good metaphors for bitcoin because there is no parallel. We have never done this before. We fall into these traps of trying to extrapolate from our previous experience, and fall short. Disruptive technologies do this. In an incremental technology, if you take what you currently understand and then just use a milligram of vision and extend it just a tiny bit, you understand the new technology because it really is just a slight extension of the past. Bitcoin is a radical break from the past, so understanding the way traditional money works doesn't help you understand bitcoin. If anything, it hinders your understanding of bitcoin. The people who understand bitcoin the least are monetary economists. They cannot wrap their heads around it. They will write long theses on how bitcoin is not money, despite the fact that I've been living on it for years.

"Bitcoin is a radical break from the past, so understanding the way traditional money works doesn't help you understand bitcoin."

Understanding disruptive technologies is even harder than understanding incremental technologies because the most interesting things they do have no previous parallel. Think about it this way . . . Look back at *Star Trek* in the 1970s. What did they get right? They got tricorders. They got portable communicators. They got video telephony. They got all that was predictable with the technology of the 1970s. They couldn't possibly get the internet. They couldn't possibly understand the idea of networked information stores. They had fantastical computers that could talk to you, but they didn't have access to any data. They couldn't possibly predict things like social media. Most importantly, if you pay attention, you will notice something very strange. *Star Trek* doesn't have any money at all. There is no money anywhere in the *Star Trek* universe. Why is that? Because their furthest vision of the possibility of society is a society without money, a society without a language for transmitting value, which is probably the most radical departure from reality.

8.4.1. Predicting the Future

When we try to predict the future, there are certain areas that are completely dark to us. These are the areas that have never been seen before. These are the applications that we cannot imagine because, in order for them to come into being, many things have to fall into place. For the web to happen, you needed a common standardized transmission protocol. For the web to give birth to social media, you needed massive penetration of basic email and TCP/IP connections. You needed penetration of those connections on an always-on state. You needed to have mobile devices with high-density computing in the palm of your hand that were internet connected. All of those things had to come to fruition before social media was even possible.

"If you look at the internet in 1992, you think that it will replace the phone. That's the only experience that you have."

If you look at the internet in 1992, you think that it will replace the phone. That's the only experience that you have. The internet is a fancy phone. Perhaps it's a fancy phone/fax, perhaps a multifunctional printer/fax/phone. It's very fancy. So, the phone companies look at this and say, "Oh, it's a fancy phone. We can do this." They were wrong, fortunately. Otherwise, every time I went on a Skype call, there would be a little slot on the side of my computer, and I would have to deposit quarters every three seconds to make a Skype call. Fortunately, the phone companies didn't get to write the rules. They couldn't possibly predict the outcomes we saw on the internet, because most of the interesting things were not incremental improvements or extensions of the things before. They were radical departures from the past, because they created the conditions for things that were not possible before.

Let's go back to bitcoin and think about this for a second. Consider what we've been talking about: financial transactions, banking, payments. "It's a fancy credit card." "It's Paypal, basically. It's a global Paypal." But it's not. It's something completely, radically different, but we can't see where that's going to go. The applications that are going to happen on bitcoin, the really interesting applications, are those that can only happen when you have sufficient adoption and penetration of this technology—the ability to do cross-border transactions on a level that has never been done in the history of humanity before.

"Consider what we've been talking about: financial transactions, banking, payments. It's a fancy credit card. It's Paypal, basically. It's a global Paypal. But it's not. It's something completely, radically different."

Today, there are 3 billion people with no banking facilities whatsoever. Three billion more people—"underbanked," as we call them—without any access to international credit or finance. You or I can go to a brokerage website right now and within 24 hours have a US-dollar-denominated account that can trade on the Tokyo stock exchange. That is privilege. That is a facility afforded to less than a billion people in the world. One out of seven. The other 6 billion? They barely have basic checking, if that. A lot of them live in cash- or barter-based societies. So, the question you then have to ask is what happens when a farmer in Kenya who has a Nokia 1000 text-messaging phone, and suddenly that phone is a Bloomberg terminal, a loan-origination terminal, a Western Union remittance-termination terminal, a stock market, is a bank—not a terminal to a bank, but a bank, on the phone? And what happens when that is afforded to the other 6 billion all over the world.

Part of the reason bitcoin is unstoppable is because there is this great need for this technology. Banks in the developing world cannot extend services to these populations. Recently, I was talking to a banker who told me, "Half our population is 100 miles from the nearest branch, upstream, on a canoe. We can't serve them." But even the remotest village in the Amazonian basin has a cell phone tower, and someone in that village has a solar panel and a Nokia 1000 text phone. There are more Nokia feature phones in the world than any other kind of electronic device. It is the most massively produced device humanity has ever produced. Almost 5 billion people have access to cell phones. Almost 3 billion people have access to cell phones and do not have access to safe drinking water. Think about that. Cell phones are more widespread than water on our planet. What happens when each and every one of those is a banker. For me, the vision of bitcoin is not to bank the other 6 billion; it's to unbank all of us. We can do it. Banking is an app.

"For me, the vision of bitcoin is not to bank the other 6 billion; it's to unbank all of us."

8.5. Interstitial Innovation

That's just the beginning. The really interesting things in bitcoin happen in what I call "interstitial innovation"—the innovation and the gaps, the places where today's systems cannot go. Technologies have an interesting effect where they suddenly change basic assumptions. Some of the most powerful things that happen on the internet happen not just because of connectivity, but because of the marginal cost of transmitting information over distance. Before the internet, moving information from point A to point B cost a lot of money. The internet drove that cost almost to zero. The result was that millions of applications that could not happen on the previous cost basis, even if we could imagine them, suddenly became possible. Why on earth would you stream music instead of buy it and store it locally? Because it costs nothing. Once it costs nothing and you can stream music, then you suddenly realize that ownership is kind of overrated. If an entire generation realizes that, then intellectual property is kind of overrated. Bye-bye, recording industry. These effects happen because the technology changes the fundamental costs of doing things.

Let's think about what happens when bitcoin changes the fundamental cost of transacting—transacting across distance, transmitting value, recording information, and recording information in an immutable way. What happens when, for the first time ever, there is a system that can evaluate rules without human intervention and be trusted without having to put trust in any single human? In bitcoin, we call this the removal of counterparty risk. If I create a transaction and I sign it, everyone on the bitcoin network can validate that transaction independently. They don't have to ask anyone. They can go through the blockchain on their own machine, which they know is correct and true because they have been tracking it and building it based on proof of work. They can check that transaction, 350 bytes, and they can validate that transaction without asking anybody else. A self-verifying system, a system of rules that exists independent of human actors, that exists based on this network topology.

"What happens when, for the first time ever, there is a system that can evaluate rules without human intervention and be trusted without having to put trust in any single human? In bitcoin, we call this the removal of counterparty risk."

What does that mean? What does it do to commerce, to transactions? We can understand what it does to banking. We can understand that Western Union is going down hard this decade. You charge 30 percent on the poorest people in the world, you deserve to go down by disruptive technology. Last year, the CEO of Western Union said, "In the medium term, we are not worried about bitcoin." I

want that framed on my wall. It's one of those phrases, like the boss of Kodak saying things like that when Nokia took away their lunch. Kodak was the largest camera company in the world until a company that wasn't in the camera business shipped a billion cameras in one year and destroyed their industry. They never saw it coming. Nokia, by the way, is the world's largest manufacturer of cameras, by far. That's going to happen to Western Union.

That's the easy stuff. What happens when you are able to do this validation of rules without a third party? It changes several fundamental societal institutions that we have today. It changes what's called the *Coase coefficient*, which is the overhead created by organization. If we want to do something as a team, two people can do more than what one person can do. Three people can achieve even more. But there's a limit to that. Once you get too big, the communication overhead between participants in the group is greater than the marginal increase in efficiency. So, adding more people makes it worse, because the group is getting bigger too fast. Bitcoin changes that, because it now reduces the coefficient of organizing on a transactional, on a commercial, on an independent-validation basis, on an extremely large scale. We can now get about a million people, about 5,000 machines, to agree on the state of a ledger every ten minutes at extremely low cost. That has never happened before. It opens the door for things that we can't even imagine. Bitcoin is radically discontinuous from the past.

Let's take one simple example: personhood. Personhood is required for financial ownership. In order to own money, in order to control funds, in order to have a bank account, to receive a bill, to pay someone, you must be a person. Everywhere in the world in every payment and financial network that exists, people own money. They may own it in the form of corporations, but that's just people grouping together. They may use proxies, agents, things like that, but that's just people working together. Bitcoin does not require personhood. A software agent can own money. A piece of software can be autonomously controlling money without any human intervention. This is completely unheard of in the history of man. We have never seen what happens next.

Here's a little thought experiment. Let's take three radically disruptive technologies and mash them together. Bitcoin. Uber. Self-driving cars. What happens when you mash the three together? The self-owning car. A car that pays for its Toyota lease, its insurance, and its gas, by giving people rides. A car that is not owned by a corporation. A car that is a corporation. A car that is a shareholder and owner of its own corporation. A car that exists as an autonomous financial entity with no human ownership. This has never happened

before, and that's just the beginning. *Audience member gasps: "Oh shit!"*

"Let's take three radically disruptive technologies and mash them together. Bitcoin. Uber. Self-driving cars. What happens when you mash the three together? The self-owning car."

I can guarantee you that one of the first distributed autonomous corporations is going to be a fully autonomous, artificial-intelligence-based ransomware virus that will go out and rob people online of their bitcoin, and use that money to evolve itself to pay for better programming, to buy hosting, and to spread. That's one vision of the future. Another vision of the future is a digital autonomous charity. Imagine a system that takes donations from people, and using those donations it monitors social media like Twitter and Facebook. When a certain threshold is reached and it sees 100,000 people talking about a natural disaster, like a typhoon in the Philippines, it can marshal the donations and automatically fund aid in that area, without a board of directors, without shareholders. One hundred percent of donations goes directly to charitable causes. Anyone can see the rules by which that autonomous altruistic charity works. We are beginning to approach things we have never seen before. This is not just a currency.

Now, let's look at how the bitcoin community is addressing this incredible potential with their design choices and metaphors. Oh boy, it's a mess.

8.6. ATM Experience

Let's take a simple example. How many of you had an experience with a bitcoin ATM—or BTM, as it's known? How was that experience? Who enjoyed it? Nobody, that's about right. What is an ATM? ATMs have been around for 25 years now. What purpose does an ATM serve? What is its goal? *Audience member:* "It's a cash dispensary." Okay. When you interact as a person with an ATM: you have a pre-existing relationship with the bank or financial institution, you have a pre-existing balance, your primary objective is to get in, get cash, get out. Twenty seconds is too long. Three clicks is too long. The most incredible innovation in ATMs in the last 25 years has been Fast Cash. That's it. They haven't really changed much. You press a button. Now, I can get cash in one click. Wow—15 seconds, in and out. Why is this important? Because one of the primary uses of ATMs is that at 1:00 in the afternoon, 100 people line up in front of four or five ATMs in the center of town and all try to take out 20 dollars to buy lunch. You see this all around the world.

What is the purpose of an ATM? For a bank, the purpose of an ATM is reducing the overhead of having a human, and reducing the interaction to the shortest possible time for someone who has a pre-existing relationship with that bank. What does that have in common with the bitcoin ATM? Absolutely nothing.

8.7. Bitcoin ATM Experience

Now let's look at the experience of a bitcoin ATM. The average user of a bitcoin ATM is someone who has never seen bitcoin before. It is a person who doesn't understand what bitcoin is, and the ATM is their first introduction to this currency. It's a person who does not have a pre-existing relationship with anyone in the bitcoin space. It is a person who does not currently have a wallet, because they didn't know they needed one. They don't know what a wallet is, they certainly don't know it's actually a keychain. They walk up to this machine, and this machine has been designed by engineers to simulate the experience of an ATM, even though the experience shares absolutely nothing with the use case we're putting it to.

So, you walk up and the ATM tries to give you bitcoin in as few clicks as possible with a minimum amount of interaction. Is that a way to build brand loyalty? Is that a way to build user experience? Is that a way to introduce new users? I mean, it just throws it at you. You're not ready for that. *Please open your phone and display your QR code.* You're like, "What? What's a QR code? . . . Hang on, let me go to Google Play and search for 'QR code.' There's an app that scans them, . . . maybe I should use that one. Shouldn't use that one. Maybe I should use a bitcoin wallet. Oh, there are 26 of them. Which one's the best? I don't know. I'll use Circle. . . . Oh, that requires a pre-existing relationship, whoops. I'll use Coinbase. . . . Oh, that requires a pre-existing relationship, oops. . . ."

Finally, I've got my wallet and I display the QR code, put some money in, and I've got the bitcoin. What am I going to do with it? I have all these questions. Who takes bitcoin? Where can I spend this? How do I send it? How do I secure it? Will it get lost if I lose my phone? I have no clue. Why? Because this bloody infernal machine didn't tell me anything. It just threw the bitcoin at me, and in 15 seconds it's off to the next customer.

If I was designing a bitcoin ATM, first of all, I'd put it in bodegas. Secondly, it wouldn't have a lick of English on it; it would be all Spanish because I'm going to really push the remittance model. Thirdly, the first function on the ATM would be *Send Money to Mexico City*. That's it. Because I want people to use the bitcoin for something. Fourth, I'd have a big button on the front that says *Talk to a Human*. I've got an internet-connected device with a forward-facing camera and a tablet screen, and I'm not using it to do video customer service, are you kidding me? Boom: Skype. A person. "What the hell is bitcoin? Where do I

spend it?" "Oh, sir, I see that you're in the bodega on 25th Avenue. There are three stores that take bitcoin in your area. Let me show you a brief introductory video. Gather all the children in the store and we can all dance to a little bitcoin song. Let's watch another video." I don't want to interact for 15 seconds. I want to interact for two hours and get all of my friends to sit in front of the machine and watch the little bitcoin videos and learn about bitcoin. It's got pretty colors, and it tells me where I can spend it. It gives me suggestions on wallets. It can send them directly to my phone. It's building loyalty, brand, and experience. That's not a 15-second interaction. This is the first experience that many people will have with bitcoin. You have the opportunity to make this a deep, meaningful, educational experience. But you don't.

8.8. Kids Use Bitcoin

Here's another little clue, kids are using bitcoin. On average around the world, the earliest age at which you can open a bank account is 16 years old. By the time that 16-year-old goes to the bank, I want them to have at least six years of active bitcoin use in their experience. Because then, when they face their first banker, they're going to be, "Three to five days?! Business days?! What the hell is a business day? What do you *mean* you close at 5:00? I barely get off of work at 5:00. What do you mean I have to pay for you to store my money. This is ridiculous. Have you people even heard of bitcoin?!"

"For many young people, bitcoin will be their first economic experience. By the time they get to a bank, they will be done with banking in advance."

That's the experience I want. Guess what? Ten-year-olds are opening bitcoin accounts. You know why? They can go download the app on the internet, and they can be in control of money for the first time. So, you need to have the birds-and-bees discussion, but you also need to have the private-keys discussion. This is a huge generational divide. For many young people, bitcoin will be their first economic experience. By the time they get to a bank, they will be done with banking in advance. That's a huge advantage.

8.9. Brand New Tech, Same Old Terms

So, how do you appeal to a completely new demographic? Part of the trick is not trying to be a bank. Do not try to do anything related to traditional banking. All that does is pollute their mind. You want new users to have a brand new experience with bitcoin that is unlike any banking they will ever see. You don't want it to look like a checking account. God forbid you use the word "checking." Open any one of the exchanges right now—Circle, Coinbase. What is the name of your account on Coinbase? It is a checking account, and it has a balance, and it shows you a statement. Who did they hire for this design? What does the word "checking" mean? It means an account on which you can write checks. I know this is America and we're 25 years behind on fintech. The rest of the world doesn't do checks, I guarantee you. What is a check? A check is the device by which a grandma can make 20 people in line behind her in the supermarket simultaneously groan. I use it to pay my rent every month. I don't know why. I can't do it any other way. It's insane that I'm signing a piece of paper and sending it through the postal system in 2015. So that my landlord can walk it through the bank and deposit it. So that it might clear three to five business days later, after they've charged him five dollars to own his own money.

We don't really need a hard sell to make bitcoin win on the banks. All you need in order for bitcoin to win against banks is for a person to use bitcoin for a week, and then the bank will take care of the rest. They'll freeze their account, they'll tell them they're closed, they'll hold it for three to five business days. They just sold bitcoin. Banks will sell it for you every single time.

8.9.1. The Joys of International Wire Transfer

I was invited to do a talk at the Bundesbank, the German Federal Bank. They were paying me for this speaking engagement, but they didn't know how to do bitcoin, which is a real problem because I usually get paid in bitcoin. So, we agreed to do a wire transfer. It took 16 days. First, they asked for my account number. Then, the next day they said they needed the SWIFT number. By that time, my bank was closed, so I couldn't get the SWIFT number. The next morning, I got the SWIFT number and I sent it to the Germans. By that time, their bank was closed. The next morning, they used the SWIFT number and discovered it was the wrong SWIFT number. It was the SWIFT number for US dollars, not for foreign currency. So, they sent me an email, but by that time my bank was closed. The next day, I got the other SWIFT number and I sent it to the Germans, but by that time their bank was closed. They sent me the wire. My bank took one look at this wire and said, "Bundesbank. Never heard of them. Sounds dodgy. Let's freeze this for 14 days, just in case it bounces." This is the third largest central bank in the world. This is the German Federal Bank. They do not bounce checks. 14 days later—and this is the great part—they said, "Money held. Money released." They released 80 dollars of the total amount, which was a four-figure amount. 80 dollars. Why 80? What the hell is that? What am I going to do with that? Just hold all of it. Are you teasing me? This makes no sense.

8.10. The Problem with Traditional Banking Metaphors

This is what we're addressing with bitcoin. If you are introducing a new product in this market and you are a designer, which parts of this design metaphor do you want to re-use in your product? According to the bitcoin marketplace, all of them, so that you can persuade people that this is just like your bank. It doesn't have any of the good parts of a bank—like the ability to easily reverse transactions, to get a refund if you lose your private key. It doesn't have any of those. It also doesn't have any of the bad parts of banks, but we don't pay attention to that. So, we've created expectations that are entirely misleading.

"Bitcoin desperately needs design. It has been created by engineers and it is absolutely inscrutable."

8.11. Innovation, Design, and Adoption

Bitcoin desperately needs design. It has been created by engineers and it is absolutely inscrutable. But I have hope because we've done this before. I got on the internet in 1989, and at the time it was illegal to do commercial activities on the internet. It was owned by the National Science Foundation, and it was only for academics (or, let's say, 15-year-olds who happen to find the password to an academic system). At the time, DNS was still in its infancy. Most systems didn't really have DNS names assigned yet. It wasn't very well structured. A lot of the most interesting things you could only find via IP address. I walked around with a list of IP addresses in my wallet, so I had access to these things. In order to use it, it required UNIX command-line skills.

There was absolutely no way that was going to get used by my mom. My mom called me and told me her stereo was broken, and I tried to figure out why. She said, "It's displaying an error message. It's blinking at me '0:00.'" It took me a few minutes to figure out that she had pulled the plug and the clock had reset. So, the clock was waiting to be set again and was blinking "0:00." That's the person who I wanted to use the internet so we could talk, but that wasn't going to happen. It took almost exactly 20 years from the day I sent my first email to the day my mom sent her first email. In order to do so, a lot of things had to happen. Most importantly, the iPad. She was able to do it with a swipe of a finger, and that was the only thing that made it possible. There was no way *that* internet in 1989 could be used by the mainstream.

8.11.1. UX and Society

There's this fantastic outtake from a morning TV show in 1994 in which the journalists are in a huddle just before the show. They are discussing their upcoming internet story, and they're trying to get their information right. One journalist is asking the other journalists, "So, wait, the internet is the thing with the 'at' sign?" "No, no, that's email. The internet is the thing with the 'www,' with the dots and the slashes." "I thought that was the email." "No, that's the internet." "But isn't that the web?" So there's this circular discussion. A system designed by engineers. Inscrutable. Two things happened. One, we made the technology much easier to understand, much better, more polished. Another important thing happened: society moved. Today, the average person knows exactly the difference between an @ sign and a www, even though it's a horrible design. Society learned the language of the internet because it was valuable enough to learn the language of the internet.

"Society learned the language of the internet because it was valuable enough to learn the language of the internet."

While we made the internet easier, society caught up and also understood the really inscrutable parts of the internet. The same thing is happening with bitcoin. I go to mainstream conferences where they have never heard of bitcoin before and I say, "Listen, don't worry. Someone in your life can explain bitcoin to you. When they're done cleaning their room, ask them to teach you bitcoin." Their 10-year-old will understand it. I've met kids that use web-based interfaces to create altcoins of their own.

One of the interesting questions I get often is "How many coins and currencies will there be?" The answer to that is exactly equivalent to "How many bloggers will there be on the internet?" All of us. All of them. Not hundreds of coins; thousands, tens of thousands of coins. When a 6-year-old can create a coin called Joeycoin to launch in his school as a popularity contest, the fact that that coin is also global, unforgeable, scalable, and can be used internationally doesn't matter to Joey, as long as his five friends really like to use Joeycoin. Unfortunately, a competitor, Mariacoin, is launched on the scene, and an old-fashioned currency war starts. This is going to happen. Part of the reason we know this is because children create currency. You leave children in a kindergarten by themselves, and they will invent currency—rubber bands, Pokémon cards, little cubes. They will start hoarding, trading, exchanging for favors, and then eventually getting into a fight over their imaginary currency that they just invented. This is a human

experience.

We just invented the world's most awesome currency. Your job now is to create the right design metaphors to make it work for everybody else.

Thank you.

Chapter 9. Money as a Content Type

Bitcoin South Conference; Queenstown, New Zealand; November 2014

Video Link: <https://www.youtube.com/watch?v=6vFgBGdmDgs>

Good morning, everyone. What I want to talk about today is a new topic I've been working on: money as a content type. Bitcoin has introduced a fundamental transformation in how money is going to be viewed in the future by making money completely independent of the underlying transport medium and turning it into a stand-alone content type.

What do I mean by that? A bitcoin transaction is a signed data structure that can be executed anywhere in the world. A lot of people think that a bitcoin transaction has to be transmitted on the bitcoin network. That's not true. A bitcoin transaction has to reach the miners and be included in a block, but it doesn't need to be transmitted over the bitcoin network. There's nothing special about the bitcoin network. It just forwards transactions and blocks. A transaction can be transmitted over any form of communication medium.

One of the magic things about bitcoin is that the transaction doesn't incorporate security mechanisms itself. The security is in the proof of work provided by the miners, and the digital signature on the transaction is put there by end users with keys that they store. There's nothing sensitive or secret in the bitcoin transaction. Let me explain what I mean by that.

9.1. Credit Cards: Insecure by Design

If I go to a merchant today using a point-of-sale system and a credit card, what I am transmitting to the merchant (through a long series of intermediaries) is the credit card number, expiry date, and CCV2 code on the back of the card. I'm actually transmitting the secret keys. I'm transmitting the access codes to my account. That information is sensitive. If that information is captured, my account can be compromised. I can be charged again and again, either by the merchant or one of the intermediaries, or any hacker who has taken this information from any of the intermediaries. My credit card information needs to be very carefully protected.

From the moment the credit card comes out of my pocket until the money is in the merchant's account, it is transported across the network in a series of virtual armored cars. There's encryption from the point of sale to the merchant's back end. From the merchant's back end, encryption through to Visa for batch processing. From Visa, encryption through to the originating bank and to the destination bank, encrypting this token at every step of the way because it is the secret key. If that encryption fails at any point in the chain, the security of my credit card is compromised.

That credit card is also stored at many of the points of transit. It's stored for historical purposes. Which is a terrible idea because that creates a centralized treasure trove, a stash for hackers to attack. We've seen this happen again and again. In the US, Target and Home Depot, two very large retailers, have had incidents where they've had 50 to 60 million credit cards stolen. JPMorgan Chase had 75 million accounts compromised recently. All of these things are not happening because these companies are delinquent in protecting credit cards.

"There are really two types of companies out there: those that have failed to take the necessary action to secure the credit cards that you entrusted them with; and those that will soon fail to take the necessary security action to protect the credit cards you've entrusted them with...Credit cards are broken by design because the token itself is the secret key. If you transmit that token, you expose your entire account to risk."

There are really two types of companies out there: those that have failed to take the necessary action to secure the credit cards that you entrusted them with; and those that will soon fail to take the necessary security action to protect the credit cards you've entrusted them with. You've either been hacked or you will be hacked—those are the two categories. Nobody's immune to this. No one can invent a way to protect millions of secure access tokens from motivated attackers. It's impossible to do. We don't know how to do it. There is no

information security trick that can protect for all possible types of attacks. Credit cards are broken by design because the token itself is the secret key. If you transmit that token, you expose your entire account to risk.

9.2. Bitcoin Transactions: Secure by Design

Bitcoin is fundamentally different. What I'm transmitting is not the key, but simply a signed message. It is an authorization. That authorization has two external references: (1) to where the money's coming from by referencing an unspent output on the blockchain, and (2) a reference to where I want to send the money — by creating a new encumbrance, a new limitation on who can spend the money, usually a public key or bitcoin address. That transaction contains no sensitive data. If you steal the information in the transaction, all you know is which address the money came from, which address the money's going to, and how much. That's it. The signature reveals nothing. The addresses reveal nothing. There are no identifiers. You could take the transaction and print it out. You could post it on a billboard. You could shout it from the rooftop. A bitcoin transaction can be transmitted over completely unsecured Wi-Fi. By smoke signal. By light signal. With carrier pigeons. It doesn't matter. Nothing in that message can be compromised.

"A bitcoin transaction can be transmitted over completely unsecured Wi-Fi. By smoke signal. By light signal. With carrier pigeons. It doesn't matter. Nothing in that message can be compromised."

9.3. Money as a Content Type

Most people don't realize what it means to convert money into a content type. We've taken the transaction, which is just 250 bytes, and we've separated it from the transport medium, so it doesn't depend on any underlying security. We've made it stand alone so that it can be independently verified by any node that has a full copy of the blockchain. Independently verified as spendable, authentic, and properly signed by *any* system that has a full copy of the blockchain—in fact, even by systems that only have a partial copy of the blockchain. That transaction can be verified in seconds. All it has to do is reach one node in the network that can talk to miners. That's it. Once it's injected into the bitcoin network and once it propagates, you can be almost certain that the transaction will be included eventually and will become valid. If I look at any transaction, I can calculate if it has sufficient fees, and then I can make certain assumptions about how miners are going to treat that transaction because I know the rules by which they operate on a consensus network. I know that once the transaction is propagated enough, it will appear in a block near you, soon.

9.4. Stopping Bitcoin Transactions Is Impossible

There's nothing magical in a bitcoin transaction. Let's think about this for a second. How can you encode 250 bytes and transmit them across the network?

Someone recently asked me, and I get this question a lot, "Can't tyrannical governments block or ban the transmission of bitcoin transactions?" The answer is *no*, but I don't think people quite understand *why* the answer is no. I'll give you a couple of theoretical examples to show what I mean.

9.4.1. Transmitting Bitcoin Transactions via Skype as Smileys

My first ridiculous example is the encoding of bitcoin transactions as emoticons or smileys in Skype. Skype has a 128-character emoji alphabet which allows you to send various frowny faces, smiley faces, thumbs up, thumbs down, sunny days, beating hearts, birthday cakes—you know, all of those kinds of things. Now, let's look at that from an information-content perspective. That's a character set, right? If I'm a computer scientist, I'm going to look at that and say, okay, I now have an encoding scheme. This would allow me to send a 250-byte transaction in about 500 characters. 500 smileys. A bitcoin transaction is smileys.

I can literally mathematically write a little script, it's two lines of Python probably. If you're really efficient, it's probably one line. No libraries needed. In the script, I can take the hexadecimal representation of a bitcoin transaction and encode it in emoticons. I can then copy that into a Skype window anywhere in the world. As long as the recipient who receives that string smileys types it into a decoder script and then simply injects it into the bitcoin network, that transaction will go through. The recipient could be a robot. The recipient could be an automated listening station that is designed to decode smileys into transactions and transmit them onto the bitcoin network.

Now, explain to me how anyone can make that stop, other than by shutting down Skype. If they shut down Skype, I'll use Facebook. If they shut down Facebook, I'll use Craigslist. If they shut down Craigslist, I'll put my transaction in a TripAdvisor review. If they shut down TripAdvisor, I'll post it as a comment in the history of a Wikipedia article. If they shut that down, I'll post it as the background of a JPEG image in my holiday snapshots.

"Money is now completely disconnected information content."

Money is now completely disconnected information content. There is absolutely nothing you can do to stop information from traveling from anywhere in the world to anywhere in the world when you have an abundance of fully interconnected multimedia communication mechanisms as we do today.

9.4.2. Transmitting Bitcoin Transactions via Short Wave Radio

Let's say we didn't have the internet. I came up with an even more ridiculous harebrained scheme, which is the transmission of bitcoin transactions over shortwave, frequency-hopping, burst radio. This is if you want to go completely guerrilla-style.

During the Second World War, in occupied France, the Allies dropped thousands of shortwave radios — complete kits with little parachutes — from airplanes, so that Partisans on the ground could hide these in barns, in tree hollows, in abandoned buildings, under bridges, and use them to communicate with various Allied command centers around Europe, from right under the nose of the occupying Nazi force. One of the things about shortwave radio is that not only do you have enormous range, but you can also, in certain frequencies, bounce off the stratosphere. At the time, they used this for voice communication or coded numbers communication, Morse code and various one-time pad encryption schemes.

Today, I can get a kit that allows me to connect a very simplistic shortwave radio transmitter to my laptop via USB. Now all I need is an antenna. The nice thing about that is that with shortwave radio, an antenna consists of a sufficiently long piece of metal — a railway line, a clothesline, a broken-down electricity line, a fence line, a razor-wire fence. Which, I've noticed here in New Zealand you have lots of. It's right around those fuzzy white things that are everywhere — the sheep.

Now, the transmission of a bitcoin transaction involves plugging in a laptop, attaching it to a fence post, pressing "enter," and transmitting a burst transaction for 25 seconds. As long as there's a receiving station somewhere within the surrounding thousand miles that is connected to the bitcoin network — and you can hide the receiving station anywhere you want, it's a passive listener, it can't be triangulated — that listening device can inject the transaction into the network. If I'm the guerrilla and I want to buy something, I construct the transaction offline, and when I'm ready, run out into the middle of the field, clamp my transmitter onto a clothesline, press "enter," transmit for 25 seconds, pack up my gear, and disappear into the forest. How the hell do you stop that? You don't. That's the simple answer, you don't. But that's just the beginning.

9.5. Separating the Medium and the Message

Once you realize that money has become a content type, that transactions have been disconnected from the medium, some really important secondary characteristics emerge. You see, the medium is the message, as someone famous once said. The primary reason the medium is the message is because the medium constrains, transforms, and in many cases, distorts the message.

When your medium is TV, your message is 18 minutes long, interrupted by advertising slots. That is your message; there is no other format you can fit there. So, you make a message that fits that medium. And you start assigning the value of your message based on the mistaken assumption that it is equivalent to the cost of production. TV, for example, imposes a certain cost to producing video. People who are in that business make the mistaken assumption that the cost of producing TV is the same as the value of that show. The more you spend on it, the more valuable it is.

You can imagine their horror when something like YouTube comes along and drops the cost of production to zero. What do you think is the immediate assumption that people make in that industry? If the cost is zero, then the content is worthless. That is a fundamental misunderstanding of what happens when you separate the content from the medium. By separating the message from the medium, your perception of value shifts from the cost of production to the value it has to the consumer when they consume it.

"When the cost of printing is astronomical and the means of printing are available only to a select few, the only thing you print is Gutenberg Bibles."

Let me give you an even older example. When the cost of printing is astronomical and the means of printing are available only to a select few, the only thing you print is Gutenberg Bibles. The medium defines the range of expression of the message, and constrains it only to the most grandiose and important messages that society has. It limits the range of expression by imposing enormous costs of production.

What do you think Gutenberg would have thought of Twitter, which takes the cost of production to zero, makes it available universally, ubiquitously, and for free. You go from printing the Gutenberg Bible to responding to a tweet with one of my favorite expressions, the three-character opinion "SMH" — which means "shaking my head." When "Professor Bitcorn" says, "Bitcoin is going to zero," I can express my entire range of opinion and thoughtful analysis as *shakes head with facepalm*. Three characters, and I have expressed my opinion to the world.

If you look at that from an objective perspective, surely that message is worthless. When you make the mistaken assumption that if the cost of production is zero, and the message appears trivial on its face, then the entire combination of medium plus message must be worthless, must be trivial, must have no value — that's a mistake that people have made at every turn in history.

When Twitter first came out, people assumed it would only be used for the trivial. And yet, a year ago I was watching *CNN International* covering the Egyptian revolution, and they were live-streaming tweets from Egyptian revolutionaries on the streets of Cairo, giving live reports about what is happening minute-by-minute. CNN anchors are doing nothing. They're pointing at the screen and saying, "Look, we have another tweet. And here's another tweet from someone we don't know. Here's another tweet." They've been reduced to the role of a TV show model saying, "And this wonderful refrigerator will be yours if you win the prize behind door number one." I find it extremely gratifying to watch one of these talking heads, like Anderson Cooper, basically reduced to reading tweets off a screen.

Because they mocked it. They made the mistaken assumption that if the cost of production is zero, the value of the message is zero. They confused the medium for the message. They made the mistaken assumption that their control over the medium was the source of quality. And long after quality disappeared, they clung to control and thought that control was the only way to achieve quality, and if you removed control, you removed quality. That is stinky, unabashed elitism at its absolute worst. It assumes that the gatekeepers are the source of quality, when all they are is gatekeepers. They assume that the fact that they have the expensive medium means that the message is worth listening to.

"They made the mistaken assumption that if the cost of production is zero, the value of the message is zero. They confused the medium for the message. They made the mistaken assumption that their control over the medium was the source of quality. And long after quality disappeared, they clung to control..."

The moment you tear that message away from the medium and you open it up to an entire range of expression, yes, it will express the most trivial messages of your culture, including "SMH." But it will also express the most interesting messages of your culture, eventually.

Today in US schools, children read *The Federalist Papers*, which are letters of correspondence exchanged between Thomas Jefferson, John Adams, Benjamin Franklin, and many of the other founding fathers. In 100 years, people will be reading *The Federalist Tweets of the Cairo Revolution*. That's not an insane idea. That is the path of human civilization. We've seen this happen again and again.

Now, they mock Twitter as trivial because they don't understand the distinction between message and medium. TV was once mocked as a trivial pastime because it obscured the art of cinematography. Cinematography was a trivial pastime because it cheapened and vulgarized the art of the theater. The theater was a vulgar and cheap pastime of Victorians because it trivialized the great dramatic plays of the Romans and the Ancient Greeks. You keep going down this path and you'll eventually arrive at Aristotle saying that philosophy is dead because nowadays the kids all want to watch dramatic presentations instead of reading their philosophy books. He probably complained about their long hair, too. Every generation mistakes the medium for value and considers the next iteration of the medium—that widens access, that opens availability, that broadens the range of expression—they consider that medium trivial, vulgar, cheapening the message.

"Every generation mistakes the medium for value and considers the next iteration of the medium—that widens access, that opens availability, that broadens the range of expression—they consider that medium trivial, vulgar, cheapening the message."

What they don't understand is when you cheapen the medium, you release the message and you elevate it. You are able now to express a broad range of messages. Yes, the first ones will be trivial. The reason they'll be trivial is because the previous medium didn't allow for that expression. It didn't have within it the ability to have that expression. Yes, you will have the "SMH." You'll also have live tweets from the Cairo revolution. By the time they figure that out, the new medium *is* the quality message. Then, we can turn around and call the next one vulgar and cheap.

9.6. Money is the Message, Now Freed from the Medium

Money is a content type, and we just wrenched it free from the medium. The medium has been a series of interconnected networks that segregate money by size and recipient. We have payment networks for small money. We have payment networks for large money. We have payment networks for fast money. We have payment networks for slow money. Payment networks for businesses to pay businesses. Payment networks for governments to pay governments. Payment networks for consumers to pay businesses. Payment networks for consumers to pay consumers. Oh wait, we don't really have those. We don't have payment networks for consumers to pay consumers. We don't have payment networks to do small payments because the traditional medium does not allow that range of expression.

"Money is a content type, and we just wrenched it free from the medium."

I cannot send you 20 cents across the world, from one individual to another individual, because the medium constrains the message. The cost of production does not allow me to express that range of transactional expression. But now we have separated the message from the medium. We have created money as a content type. That money is now able, at near zero production cost, to express the entire range of transactional expression—from the tiny to the enormous, from consumer to consumer, from government to government.

What happens next? The gatekeepers tell you that this network is not serious. The gatekeepers confuse their payment-network cost for the value of their service. The gatekeepers of the old payment networks will tell you that this new form of payment is vulgar and cheap. It is something that is only used for trivialities. All of the very serious people will remain on the solid, quality payment networks of the past. Because if they can control and restrict the range of expression, they think that means it's quality. It's not. It's just an inflated cost of production. It's bare naked elitism at its worst. They cling to the medium and fail to see that now the message can be transported over any medium at zero cost, instantaneously.

What is the first use of this new model? What is the first use of this new messaging medium? Now we can send trivial payments. I get tips on Twitter. That's a demonstration I can make that clearly shows people the difference. I can do something I could not do before. But to most people, that's trivial. To most

people, the fact that I'm showing them the bottom of the range of expression simply reinforces the idea that this is a cheap and vulgar medium. What they fail to grasp is that this medium is not just for the trivial; it spans the entire range of transactional expression from the trivial to the enormous.

"The blockchain can encompass the entire range of transactional expression, from the 10-cent tweet to the \$100 billion debt settlement."

One day, a country will pay its oil bill on the blockchain. One day, you might buy a multinational company on the blockchain. One day, you might sell an aircraft carrier, hopefully for scrap metal, on the blockchain. The blockchain can encompass the entire range, from the 10-cent tweet to the \$100 billion debt settlement. We just haven't noticed yet. It can do so without any constraint imposed by the underlying medium. This isn't just a matter of the fact that the transaction as a content type can be transported over Skype smileys. That's simply a symptom of the fact that we have released all of the constraints of the underlying transport medium. We have made content king.

9.7. Grand Arc of Technology

When content begins as the domain of exclusivity, elitism, and limited access, it is used by grandmasters to create masterpieces. The Gutenberg Bible. The first photographs. The landing on the moon, televised for the first time. The great movies of the past. Masterpieces made by grandmasters.

Then the medium changes because the technology becomes more available. People start using it for a broader range of expression, but the gatekeepers still cling to the old ideas. They still try to do the grandiose with their medium. They print hardback, heavy, leather-bound books—*Principia Mathematica*. Then the medium opens up again and things become softcover, and photographs become available to the everyday person in 24 exposures. The gatekeepers of the past still cling to the past, but now they can't really pretend that it's grandiose, so they just do grandstanding. They say, "There's a certain *je ne sais quoi* to film." "There's a certain quality to vinyl that CDs will never capture." "A TV anchor really has authority. Don't you remember Walter Cronkite?" "A newspaper is the source of authoritative opinion, and it really is worth the paper it's printed on." Grandstanding. The grandiosity is gone. The quality is gone. Now, it's just a matter of clinging to the control and pretending that control is still quality.

Finally, in this grand arc of technology, the technology reaches the final stage. In that final stage, the only people who still believe it's grand are grandparents. In the grand arc of technology, what started out as a masterpiece is now only consumed by those in the last stages of their lives. The first checks written out were used by royalty to fund great ventures like the East India Company to open the spice roads and trade routes to the East. In those days, only royals had checkbooks. Today, if you go into a supermarket and the grandmother, bless her heart, in front of you in the line opens up her purse and pulls out the checkbook, 15 people in line are going to groan audibly as they realize it's going to take 15 minutes to write out that transaction. There's nothing left of the grandiosity of funding the East India Company when you're buying beans and toast with a checkbook in a supermarket. It's the final stage.

The only people watching *Fox News* now are grandparents, because we all get our news on the internet. What was once trivial is now our source of authoritative news and information. You can't explain that to the old guard. We read our books electronically. Some people say, "There's something about the feel of paper." Yes. It's too heavy to carry 20 books in your bag, and I read 20 books in four or five weeks, so I need to carry that many. There's nothing about

the feel of paper; that's clinging to the past.

"As we move into this world where money is a content type, the gatekeepers of the old payment systems will cling to the illusion that traditional banking is quality. That the gatekeepers are the quality. But that's not where the quality is."

As we move into this world where money is a content type, the gatekeepers of the old payment systems will cling to the illusion that traditional banking is quality. That the gatekeepers are the quality. That the quality is inherent in the gatekeeping—in the control, in the censorship, in the limitations. But that's not where the quality is. We're moving on and opening up the range of expression that is possible with money to unimaginable levels, to things that have never happened before. They'll still cling to their ideas of grandiosity: the great old banks with the vaulted ceilings and the chromed vaults that are empty, where you can get guided tours on Sundays, to look at what banks used to be like. You can go into cities around the world and the great vaults of the great old banks are now bars where you can get a cocktail in the vault, because banks can't even afford to have those buildings anymore. They serve no purpose other than grandiosity. They'll still try to persuade you that through their control, they protect you from evil, from terrorists, from money launderers. All they're doing is protecting their own incumbency from competition.

We have now separated the message from the medium. Money is now a content type, and we're never going back.

Thank you.

Note from Andreas to the reader: In this talk I foolishly attempted to improvise math in my head while delivering the talk. I am not very good at math. Turns out I am even worse at improv-math. None of my bad math changes the point I was making, but it's been edited out for accuracy and to protect my ego. Ssssh! Don't tell anyone I suck at improv-math.

Chapter 10. Elements of Trust: Unleashing Creativity

Blockchain Meetup; Berlin, Germany; March 2016

Video Link: <https://www.youtube.com/watch?v=uLpSM3HWU6U>

Today, I'm going to talk about the chemistry of money, specifically the chemistry of bitcoin. This is one of the aspects of bitcoin that makes it so exciting and so interesting. It's one that most of us don't even notice until we study bitcoin for a year or two. Bitcoin is a bit like an onion. You have to unwrap it. As you unwrap it, you find one more layer. I started five years ago. I am still unwrapping. I am finding more and more things that surprise me every day about bitcoin.

10.1. The Illusion of Senders, Receivers, and Accounts

When I first encountered bitcoin, I was surprised to see that it looked like a relatively familiar banking system. I visited well-known bitcoin sites, like blockchain.info, and I could see transactions. I clicked on the transactions and I could see a sender, receiver, and account. I thought, *This is pretty familiar. Banking. Great.* Then, I decided to look at the source code and see how it worked.

As a computer scientist, I figured I'd read the source code, and I'd try to understand how the system does these things. But when I searched the source code for sender, receiver or account, I didn't find anything. Because none of those things actually exist in bitcoin. That really surprised me because when I looked at the source code, none of the things that I expected to find there were actually there. You'd expect that a banking system, as it appeared to be, had been designed to do certain things in a very specific way. Bitcoin isn't like that. It's not like that at all.

"When I searched the source code for sender, receiver or account, I didn't find anything. Because none of those things actually exist in bitcoin."

How many of you have looked into the source code or understand the technical underpinnings? A few people in this room. When you dig through the code, you find there is no balance, no sender, but there is UTXO *unspent transaction outputs* and there are inputs. But those inputs don't really correspond to senders. And a transaction has outputs, which don't really correspond to receivers. Suddenly, you realize what you're looking at is almost this quantum or atomic nature of bitcoin.

10.2. Bitcoin's Atomic Structure

In chemistry, we have elements like copper, iron, and helium. Chemistry gives you this enormous complexity of things that you can combine to make interesting things. Like people. And toasters. But when you dig into the chemistry, you realize copper isn't a thing. Copper is a pattern of protons, neutrons, and electrons. There is no copper. One proton is the same as another proton; it can just as happily be part of helium or copper, it doesn't care. There is nothing about that specific proton that makes it part of copper.

Chemistry is one layer, but underneath that is atomic physics. That layer is very simple. It has a handful of elements. This handful of just a few elements makes up all of the chemistry we know, 100+ elements in nature that all have unique and different properties, that are completely different. Some of them are liquid, some of them are metals, some of them are gases. They behave differently. Some are acidic, some are not. But none of that is their basic makeup. These are just patterns.

Bitcoin has this fundamental atomic structure, this elemental structure. The elements of bitcoin are the components of transactions and the elements of the scripting language. Those elements have nothing to do with traditional banking. There are no accounts and balances and senders and receivers. Instead, bitcoin's elements are looking for fundamental mathematical properties and cryptographic properties — such as whether a hash is equal to another hash, whether an elliptic curve signature matches another elliptic curve signature, manipulation of numbers, etc., etc. What you see on the surface — the transactions — are just constructs. They're a specific way of mashing up the elements that creates something that kind of looks like a bank. Which is great because if you're new to bitcoin and someone tells you, "Well, there is an account, a sender, and a receiver," you think, *Okay, I understand this.*

"What you see on the surface — the transactions — are just constructs. They're a specific way of mashing up the elements that creates something that kind of looks like a bank."

Then you learn that you have a wallet, but your wallet doesn't have coins, it has keys, and those keys could be copied, and now you're thinking, *You're losing me. This doesn't quite match my experience.* Things get complicated because bitcoin isn't what you think it is. It's a platform. It's not a payment network. It's not a currency. It's not a banking system. It's a platform that guarantees certain trust functions. If you happen to have a platform that guarantees certain trust functions, one very useful application for that is to build a currency and a

payment network, but you can build more things.

"Bitcoin isn't what you think it is. It's a platform. It's not a payment network. It's not a currency. It's not a banking system. It's a platform that guarantees certain trust functions."

10.2.1. Building Blocks of Lego

When I was a child, my favorite toy was Lego. The reason my favorite toy was Lego was not because of what was on the box. Because I did not build what was on the box. If the box had a red firetruck, I would build a dragon, or a hippopotamus-giraffe, something that didn't exist or some strange idea that I had. That's what I liked about it. I could take these basic building blocks, and I could build whatever I wanted.

From an abstract perspective, Lego is messy. And the thing I built didn't quite look like a firetruck or a spaceship. If someone had given me a toy that was a firetruck, like a plastic-injected, smooth-edged, completed red firetruck, it would be the perfect firetruck. But it could only ever be a firetruck, and 20 minutes after I start playing with it, I am bored. Because my smooth, rounded firetruck that is only a firetruck, is a perfect firetruck. But it could never be a hippopotamus-giraffe or a tomato or a spaceship. But Lego allows more.

10.2.2. Building Blocks of Cooking

As I grew older, I started getting into cooking as a hobby. What I loved about cooking is that it is the perfect combination of art and science. If you fundamentally understand how the ingredients work, how they behave, and how the chemistry changes when they're combined or when you add a catalyst like salt or when you apply heat to them, then you can create. You can create almost anything. As long as you understand how the ingredients work, you can execute and deliver anything you want to create.

10.2.3. Building Blocks of Creativity

Bitcoin encompasses that elemental nature. It doesn't give you a final result. It gives you a set of ingredients and a recipe. It gives you a set of Lego blocks and a photo on the box that looks like a red firetruck. When we present that to the world, the financial companies look at that and say, "Well, your firetruck has sharp edges and it's made of silly little blocks." In bitcoin, we take the ingredients, we put them together and we've made a banking payment system. The banks look at it and it's as if they're saying to us, "Your burger is okay but at McDonald's we can make it in 45 seconds and we can sell a billion of them. So, why do you need a chef, ingredients, a recipe, if you can just churn out a billion of them?" They're missing the point.

"Bitcoin encompasses that elemental nature. It doesn't give you a final result. It gives you a set of ingredients and a recipe."

The point is not generating a billion copies of the same inferior product. The point is not getting the injection-molded plastic red truck that I am going to be bored of in 5 seconds. The point is unleashing my creativity by giving me the tools and the elements I need to build something unique.

I didn't build a burger as fast or cheap as McDonald's, and my little red firetruck isn't as smooth as the molded copy. But I can make albondigas with red tomato sauce. I can also make a hippopotamus-giraffe. You can't do that with a prefabricated toy. You can't do that in your McDonald's kitchen. I've unleashed my creativity.

10.2.4. Building Blocks of Bitcoin

We're beginning to see people realize that bitcoin is a set of ingredients and you have one recipe, but you can make a different recipe. People are now trying to recombine these ingredients.

We're building crowdfunding projects by combining atomic transactions and input-versus-output sums and digital signatures. By combining these ingredients, we can create a single transaction that can be funded by multiple people, but the transaction will only be valid if the threshold funding is met. Those are the same elements I use to make a payment of a dollar to you over bitcoin's payment network, but you can recombine them differently and now you've got a crowdfunding platform.

We're building payment channels by combining 2-of-2 signatures, multisignature, with transaction time locks. This allows us to charge for video-streaming by the second. That's a whole new recipe.

We're building on top of payment channels. By taking them and adding a new ingredient, Hash Time Locked Contracts, we can connect multiple channels together. Then we've got Lightning Network, and that's a new recipe that nobody has ever seen before.

"We're trying to unleash the creativity of an entire generation. We're building a system, on top of which a thousand applications that require trust can be built."

The banks are saying, "Your truck has sharp corners and your burger is too expensive and took more than 45 seconds." What they're really saying is, "Your transaction fees are too high and you're too slow and you can't possibly scale." *They're missing the point.* The point is that we're not trying to sell a billion burgers at 45 seconds each; we're trying to unleash the creativity of an entire generation. We're building a system, on top of which a thousand applications that require trust can be built.

10.3. Focus-Group Economies

When you have the ingredients, when you have these basic elements, what recipe you build is entirely up to you. Because when they build the little red firetruck, they create an entire factory that can only do little red firetrucks. I'm sure they'll tell you, "Listen, our statistics say that 95 percent of children want a little red firetruck. We have tested this with focus groups and the marketing teams. We can produce them by the millions. They only cost 3 cents. They have a very small amount of lead paint and poisonous, toxic, carcinogenic hydrocarbons, not a problem. We can do that very cheaply and very profitably." And they can only build firetrucks.

When you build a kitchen like McDonald's, you can churn out burgers every 45 seconds, but you can't make albondigas. You can't make something else. You are streamlined to do one thing and one thing only, and as long as that serves your profit line, it's okay. Because I am sure you focus-group tested it to make sure that is what everybody wanted.

That is a terrible way to build an economy. That's a terrible way to build a financial system. That's a terrible way to build a payment network.

10.4. Banking Privilege and Surveillance

Effectively, what the banks are saying to us is, "We focus tested this. What people want is the ability, instead of swiping their Visa card, to wave it over the reader, saving almost two seconds and reducing their effort by at least four calories. I mean, we could deal with the 4 billion people who have no access to banking or clean water. We could deal with the fact that our world is a fragmented mess, where the vast majority of humanity have no access to financial services. Or, we could reduce the shopper's effort and make a swipe card into a float card.

We could face the fact that the reason more than 4 billion people are unbanked is because we require everyone to be identified on every side of every transaction, so that we can build a totalitarian surveillance system that the Stasi would be jealous of, to monitor every financial transaction from every corner of the planet. Because we have persuaded ourselves that our bourgeois sense of security will be protected, not by solving poverty, and not by reducing, perhaps, the bombing of other countries, but instead, by watching everyone all the time when they buy a burger—just in case.

"We could face the fact that the reason more than 4 billion people are unbanked is because we require everyone to be identified on every side of every transaction, so that we can build a totalitarian surveillance system that the Stasi would be jealous of...Because we have persuaded ourselves that our bourgeois sense of security will be protected, not by solving poverty, and not by reducing, perhaps, the bombing of other countries, but instead, by watching everyone all the time when they buy a burger—just in case."

We subject ourselves to this mechanism that has now streamlined itself, and like the factory that can only produce little red firetrucks, this is a system that can only deliver privileged financial services for a tiny elite sliver of the population worldwide, with totalitarian surveillance tied up in regulations of each country, with barriers on the borders not permitting international trade. A financial system where the government can apply pressure to stop you trading with WikiLeaks, because they don't like them, but you can still send donations to the Ku Klux Klan—and that's not a joke. That's exactly what happened.

They have built a system that can only do one thing: enslave us. That can only do one thing: impoverish us. That system removes freedom in the most efficient possible way to deliver profits. That system is broken, and it doesn't scale. But if that is what you're trying to do, it's the most efficient you've ever seen.

By comparison, the crazy little mishmash system that we've built with bitcoin, that's wrong and it's slow and it can't scale. It's inefficient and it's not as serious

and sophisticated as the international banking system. But it delivers freedom and it allows us to unleash creativity.

Thank you.

Chapter 11. Scaling Bitcoin

Bitcoin Meetup at Paralelni Polis; Prague, Czech; March 2016

Video Link: <https://www.youtube.com/watch?v=bFOFqNKKns0>

11.1. Stories of Scaling

Today, I'm going to talk about scaling. A lot of you probably have noticed that there is a very interesting debate in bitcoin today about how to scale bitcoin. That's the topic I want to address, not from a technical perspective but from a broader perspective, to try to understand what it means to scale.

11.1.1. Usenet Will Destroy the Internet

Gather around and we will talk about a long time ago. It was 1989 and the internet was dial-up. Not just the connection of users to the internet; in most cases, the backbones to the internet were dial-up. Between universities, between research stations, there were a few permanent high-speed connections — 256 kilobits, 512 kilobits. But the internet was mostly dial-up. Email had not yet really started to take hold, but there was a special place on the internet called Usenet. Usenet was a system of discussion groups where you could post a message in text and other people would see it and then they would respond.

This was not instant messaging. This was *slow* messaging because, in order for Usenet to work, all of the messages had to be transmitted via dial-up systems and propagated from node to node in a system called *store and forward*. You would post a message and it would take between 24 and 48 hours to reach everyone. Then, they could respond and it would take 24 to 48 hours for you to see their response. Today, we would compare that to trying to communicate with Matt Damon on Mars, like in *The Martian* movie.

At that moment, there was a big conversation among the engineers of the internet because Usenet was getting very popular and it was getting very big. Kilobytes and then megabytes of text information needed to be transmitted. At first, it would take about 30 minutes on a dial-up connection to get all of the Usenet messages for a day. Then, as the system became more popular, more messages meant more data and more time. Soon, it was taking one hour, two hours, and three hours. And the experts predicted the end. They said, if you draw a point at where we are today and another at where we were six months ago, and connect them in a line, very soon it will take 26 hours to transmit one day's messages and then we have a problem because we only have 24.

So, what happens then? The internet will collapse! Clearly, it can't scale. It won't possibly scale.

11.1.2. Alt Groups Will Destroy the Internet

At the time, there were two parts to Usenet. There was the regular part of Usenet, which contained very carefully structured groups for academic discussions, and then there was another little part of Usenet called *the alt*, the alternative groups. The alt was optional. As a Usenet provider, you could carry alt if you wanted to but you didn't have to. The really interesting providers offered the alt groups. Of course, all of the interesting stuff was in the alt groups: some of the early amazing groups, alt.folklore.computers, alt.security, and of course, like everything else that's been driving scale on the internet, alt.sex.

These alternative groups, being optional, were the focus of this great debate. Should we carry them? Because at this point we started seeing the world's first spam. I remember receiving the first spam. It was a message by a couple of lawyers that was posted to every Usenet group. You did not do that. That was not cool. A thousand people told them it was not cool. That was the first internet backlash.

The discussion was, do we carry alt groups? Because if we carry alt groups, the internet will surely melt down and there is no way it could ever scale. If this becomes popular, people will discuss more, and if they discuss more, we won't have enough capacity to deal with this data. This conversation lasted for more than two years. There were a few brave service providers that carried the alt groups, and they used massive hard drives—huge 5MB hard drives. Again, the main idea was, if you take the where-we-are-here and where-we're-going-up-there, we hit a wall.

"If we carry alt groups, the internet will surely melt down and there is no way it could ever scale."

So, the internet couldn't scale. That was the basic beginning of the scaling issue on the internet. It couldn't scale, wouldn't scale, clearly. Many people wrote their Ph.D. theses on why it wouldn't scale.

But of course, the thing is, networks don't scale. Networks fail to scale. Some networks fail to scale gracefully for decades, and those are the ones that succeed.

"Some networks fail to scale gracefully for decades, and those are the ones that succeed."

Eventually, we solved the Usenet problem. Digital connections were upgraded, more systems connected with leased lines and direct connections. Dial-up was gradually replaced by leased lines. People started investing in the infrastructure and we could comfortably carry Usenet. Then, people started using email. And the scaling problem returned.

11.1.3. Email and Email Attachments Will Destroy the Internet

As email became popular, it started replacing and eclipsing the size of Usenet. Now, we had an even bigger problem because people wanted to communicate directly. Now, a message didn't take 24 hours, it took two hours to cross the internet, which meant that people started having real-time conversations—well, near real-time. Email use exploded. And again, the internet couldn't scale because if you look at where email is today and where it was six months ago and draw a line, we cannot scale. The internet will melt down. People wrote more Ph.D. theses about how the internet would die under the load of email and never scale.

Gradually, we started optimizing. We solved the email problem. And when I say "we," I was just watching because I was a 16-year-old who didn't know what the hell was going on. But we as people, as humanity, we solved the problem. We scaled it. The internet failed to scale for Usenet and it succeeded to scale for Usenet so that it could fail to scale for email. Then, it succeeded in scaling for email, so some smartass went and invented MIME, multimedia internet messages, which meant that you could attach things to email. These attachments were 10 times the size of the text because people started sending bigger things, like drawings and pictures and of course, once again, sex.

So, we could scale for email but not for email attachments. Everybody was up in an uproar: "We're never going to be able to scale for email attachments. The internet will surely melt down!" Then we solved it. Until some British guy, Sir Tim Berners Lee (who then was just Tim) invented the web. Now, you could put the pictures into frames.

11.1.4. The Web Will Destroy the Internet

It was about 1992 when I downloaded and ran the first web browser, NCSA Mosaic, at my university lab. We gathered together three or four friends. We worked for hours to get NCSA Mosaic downloaded and compiled and installed. Then, we launched it and we visited the web. All of it. I can say a sentence not many people can say: In 1992, I visited the entire web in an afternoon. Both sites. Because there were two. I visited both sites, and I thought, *Oh my God. This is going to be huge! The internet will never scale. And just imagine what you could do with sex on the web!* Of course, this became *the* scaling application, as we all know. It has been driving internet development since the beginning, but we don't talk about that in polite company.

"I can say a sentence not many people can say: In 1992, I visited the entire web in an afternoon. Both sites. Because there were two. I thought, Oh my god, this is going to be huge! The internet will never scale."

The internet was failing to scale for the web. People said, "We can never do all of these images and hypertext documents. It will totally fail to scale." And more Ph.D. theses were written and more discussions were had. The internet was still failing to scale. But by now, it had been failing to scale for more than a decade, very gracefully, very successfully.

11.1.5. VOIP Will Destroy the Internet

Then, someone invented Voice Over IP. Some other people decided, why don't we just replace the entire phone system with the internet? That was a crazy idea. The phone companies then started this massive campaign to inform us of why packet-switched networks could never carry voice. They said, really, the true quality approach to voice was always going to be hierarchical switch networks owned by national monopoly telecom companies because the internet couldn't possibly scale to carry the world's phone calls.

Those same phone companies (the ones still in business) now route all of their phone calls over the internet. First, they didn't want the internet on their phone networks. Then, they allowed the internet on their phone networks. Then, they built their phone networks on top of the internet.

"First, they didn't want the internet on their phone networks. Then, they allowed the internet on their phone networks. Then, they built their phone networks on top of the internet."

11.1.6. Cat Videos Will Destroy the Internet

Then, we started sending videos. And then the internet couldn't scale again because YouTube was going to melt down the internet. Clearly, we needed some content quality and filtering because we can't allow every idiot to go and publish a video about their cat. They said, "There are already a thousand cat videos. If you draw a line from how many cat videos there were yesterday to how many cat videos there are today and if you extrapolate, by the end of this decade, there will be a billion cat videos on the internet!" Which is exactly what happened.

But we scaled. Now, we do 3D video and 4K video.

11.1.7. Netflix Will Destroy the Internet

When Netflix came along, we saw the same mistake. In 1992, when I visited the first website, my thought was, *Wow, TV is so dead because one day we will be able to transmit movies instantaneously*. If you go and say that to a respectable network researcher in 1992, they call you an idiot. Because, clearly, if we had Netflix in 1992, a single video stream to a single user would melt down the entire internet. Yet, here we are today. By the way, the internet is failing to scale for Netflix and all of the other companies that are doing live video. It will continue to fail to scale incrementally and gracefully. Soon, we'll be doing Oculus Rift holographic 3D, 4K, VR. Then, it will really fail to scale. People will still write Ph.D. theses on why the internet is about to melt down.

11.2. Scaling is a Moving Target

Scaling is a moving target. Scale defines the edge of today's capabilities. As it moves forward, capability increases. The reason for this is really simple: it's because scale is not a goal to achieve; it is a definition of what you can do with the network today. The moment you increase the capacity, the very definition of what you can do with a network today changes because somebody says, "Hang on a second. You mean I can now do x, which has 10 times more demand than what I did before? Let's do some of that." And then, you fail to scale again. Scaling is a moving target. Scale defines the edge of today's capabilities. As it moves forward, capability increases.

"Scaling is a moving target. Scale defines the edge of today's capabilities. As it moves forward, capability increases."

Bitcoin is failing to scale. If we're really lucky, bitcoin will continue to fail to scale gracefully for 25 years, just like the internet. The very same types of companies that then were saying the internet can never work for all of the email, it can never work to do quality voice calls, it can never work to do quality video, are now making the same kind of corporate arguments about why bitcoin can never do retail payments, it can never do Visa scale, it can never do global scale, and if it's actually adopted, it will collapse. Right now, there are a dozen people writing their Ph.D. theses on how bitcoin will fail, has failed, is dying, was dead, and has died again.

"Bitcoin is failing to scale. If we're really lucky, bitcoin will continue to fail to scale gracefully for 25 years, just like the internet."

There is a beautiful site called bitcoinobituaries.com where you can read the pronouncements of the death of bitcoin since 2009 — regularly, like clockwork every three to six months, major newspapers, scientists, etc., saying, "That's it. Bitcoin is dead." In fact, this has now become an amazing recruitment opportunity because all you have to do is wait for people to hear that bitcoin died, the CEO of Bitcoin was arrested, or bitcoin was shut down by Putin, and then, four months later, someone says, "You know there are some interesting new applications on bitcoin." And they go, "Bitcoin is still there?"

"Bitcoin is still there" is the marketing slogan of this community. If we can just keep doing "bitcoin is still there," people are surprised, they're confounded. It doesn't match their expectations. It's not possible that bitcoin is still there because very serious people with very serious titles, working for very rich companies, told them that bitcoin was not going to be there. But bitcoin is still

there, because we are failing to scale gracefully.

11.2.1. Fee Optimization and Scaling

When we fail to scale during a stress test or a capacity test, when the network is flooded with transactions, what happens? Some users experience a terrible situation. They do a transaction with a 0.1 millibit fee like they've always done, and it takes three days to confirm. During that time, they're freaking out, especially if they're new users. Because new users assume that the money has left their account (there are no accounts in bitcoin) and is en route to the destination account (again, there are no accounts in bitcoin), and therefore is somewhere in limbo in between. The money is really still in their account; it's just that their wallet says it hasn't been confirmed yet. It's either at the source or at the destination, atomically with one transaction. There is no intermediate state. It can't be in limbo because bitcoin doesn't transmit, it settles.

We experience these sudden problems, and some wallets behave intelligently and they increase their fees, sometimes by 100 percent. What this means is instead of it costing 4 cents to send a global transaction in seconds anywhere around the world with full censorship resistance and open innovation and open access to everyone, it takes 8 cents to send that transaction! Clearly, this is an indication, together with the people who waited three days to confirm their transaction, that bitcoin is surely dead now. And some of the developers say, "Oh, I give up. Bitcoin is dead." The newspapers write, "Bitcoin is dead. Transactions are not going through."

Transactions *are* going through. They went through for me. I was running a wallet that was intelligent; it was doing its transaction-fee calculations. What happens in the aftermath of this capacity crunch? We get better wallets.

That's really the essence of a dynamic system responding to pressure because, as we get better wallets, these better wallets calculate fees more correctly. And it's a lot easier to jam the network if there are a lot of dumb wallets doing 0.1 millibit fees, but then, all you have to do is do 0.11 millibit fees and you are king of the hill. Because the other idiots didn't update and jammed the network with their transactions. But if they're able to do 0.12 millibits, now you'll have to do 0.13. Now, we're in a race, and before you know it, you're spending 0.5 millibits, oh dear, on a transaction which of course, if you're a legitimate user, is nothing. If you're trying to jam the network, it starts getting really expensive, really fast.

11.3. Spam Transactions, Legitimate Transactions, Illegitimate Transactions

Which brings up an interesting question: What is a spam transaction? What is a legitimate transaction? What is an illegitimate transaction? There are two ways to answer this. One is a paternalistic, top-down approach that says, this is what is allowed, this is what is not allowed, and by making a list, we will prevent the network from filling to capacity. But that breaks the fundamental capability of bitcoin, which is net neutrality. Bitcoin doesn't care who the sender or the receiver is, what the application is, what the value of the transaction is. All it cares about is, did you pay the fee? If you paid the fee, your transaction is legitimate by definition because you thought it was legitimate enough to attach that fee. The very act of paying the fee legitimizes the transaction. If we start making decisions about what is spam and what is not, we are now choosing the future of bitcoin and constraining it into a set of applications that we can imagine. The brilliant person who creates the application we *can't* imagine—that may look like spam to us—doesn't get carried across the network because we made a top-down decision to say that transaction is illegitimate.

"The very act of paying the fee legitimizes the transaction. If we start making decisions about what is spam and what is not, we are now choosing the future of bitcoin and constraining it into a set of applications that we can imagine."

The other way to do this is to say, how about we use a market to solve this problem. We have a market. We have a currency. Use the market to solve this problem: allow the market to establish the minimum fee that meets the requirements of supply through the miners and their need to propagate blocks fast, and the demand of the users for the applications they care about. If you pay the fee, your transaction is legitimate. There is no spam transaction. There is no such thing as an illegitimate transaction. There are only transactions that did get mined and transactions that didn't have enough fee to get mined.

11.4. Decades of Failing to Scale

This is how bitcoin is going to play out. This is not going to be solved; we will have the scaling discussion every year for decades into the future, hopefully. Every year, we will fail to scale for the next application and succeed to scale for the previous ones. As soon as we do better, people will invent new applications and we will fail to scale again.

"Every year we will fail to scale for the next application and succeed to scale for the previous ones."

The internet: failing to scale gracefully for 25 years. Bitcoin: let's keep failing to scale gracefully, and bitcoin is not yet dead.

Thank you.

Appendix A. Video Links

Each of the chapters included in this book are derived from talks delivered by Andreas M. Antonopoulos at conferences and meetups around the world. Most of the talks were delivered to general audiences, yet some were delivered to limited audiences (like students) for a particular purpose.

Andreas is known for engaging with the audience during his presentations, much of the crowd interaction has necessarily been cut from the text. We encourage you to view the original content, if only to get an idea of what it's like to attend one of these events. All of the videos and many more are available on Andreas's youtube channel — aantonop. <https://www.youtube.com/user/aantonop>.

Below you'll find a list of the talks we've included in this text, along with locations, dates, and links to the original content.

What Is Bitcoin?

Disrupt, Start-up, Scale-up Conference; Athens, Greece; November 2013;
<https://www.youtube.com/watch?v=LA9A1RyXv9s>

Peer-to-Peer Money

Reinvent Money Conference at Erasmus University; Rotterdam, Netherlands; September 2015; <https://www.youtube.com/watch?v=n-EpKQ6xIJs>

Privacy, Identity, Surveillance and Money

Barcelona Bitcoin Meetup at FabLab; Barcelona, Spain; March 2016;
<https://www.youtube.com/watch?v=Vcvl5piGIYg>

Innovators, Disruptors, Misfits, and Bitcoin

Maker Faire at the Henry Ford Museum, Detroit Michigan; July 2014;
<https://www.youtube.com/watch?v=LeclUjKm408>

Dumb Networks, Innovation, and the Festival of the Commons

O'Reilly Radar Summit at Navy Pier; San Francisco, California; January 2015; <https://www.youtube.com/watch?v=x8FCRZ0BUCw>

Infrastructure Inversion

Zurich Bitcoin Meetup; Zurich, Switzerland; March 2016;
<https://www.youtube.com/watch?v=5ca70mCCf2M>

Currency as a Language

Keynote at the Bitcoin Expo 2014; Toronto, Ontario, Canada; April 2014;

<https://www.youtube.com/watch?v=jw28y81s7Wo>

Bitcoin Design Principles

Harvard Innovation Lab for an IDEO Workshop; Boston, Massachusetts;
June 2015; <https://www.youtube.com/watch?v=Ur037LYsb8M>

Money as a Content Type

Bitcoin South Conference; Queenstown, New Zealand; November 2014;
<https://www.youtube.com/watch?v=6vFgBGdmDgs>

Elements of Trust: Unleashing Creativity

Blockchain Meetup; Berlin, Germany; March 2016;
<https://www.youtube.com/watch?v=uLpSM3HWU6U>

Scaling Bitcoin

Bitcoin Meetup at Paralelni Polis; Prague, Czech; March 2016;
<https://www.youtube.com/watch?v=bFOFqNKKns0>

Colophon

Talks by Andreas M. Antonopoulos <https://antonopoulos.com/> @aantonop

Cover Design Kathrine Smith: <http://kathrinevsmith.com/>

Transcription and Editing S.H. El Hariry, Pamela Morgan, Maria Scothorn, Sarah Zolt-Gilburne

Copyediting Brooke Mallers, Ph.D.: @bitcoinmom

Copyright © 2016 by Merkle Bloom LLC All rights reserved
info@merklebloom.com

Disclaimers:

This book is edited commentary and opinion. Much of the content is based upon personal experience and anecdotal evidence. It is meant to promote thoughtful consideration of ideas, spur philosophical debate, and inspire further independent research. It is not investment advice; don't use it to make investment-related decisions. It's not legal advice; consult a lawyer in your jurisdiction with legal questions. It may contain errors and omissions, despite our best efforts. Andreas M. Antonopoulos, Merkle Bloom LLC, editors, copy editors, transcriptionists, and designers assume no responsibility for errors or omissions. Things change quickly in the bitcoin and blockchain industry; use this book as one reference, not your only reference.

References to trademarked or copyrighted works are for criticism and commentary only. Any trademarked terms are the property of their respective owners. References to individuals, companies, products, and services are included for illustration purposes only and should not be considered endorsements.

Licensing:

Almost all of Andreas's original work is distributed under creative commons licenses. Andreas has granted us CC-BY to modify and distribute the work included in this book in this way. If you would like to use portions of our book in your project, please send a request to licensing@merklebloom.com. We grant most license requests quickly and free of charge.

Index

A

abstract value, [Barter to Precious Metals](#)

access control, [New Architecture, New Access, Open Innovation and Opt-In Systems](#)

account, [The Illusion of Senders, Receivers, and Accounts](#)

accounts, [Fee Optimization and Scaling](#)

adoption, [Bitcoin, the Zombie of Currencies](#), [Incumbent Reactions to Innovation](#), [Infrastructure for Natural Gas](#), [Choosing Currencies and Communities](#), [Innovation, Design, and Adoption](#)

age of, [How Old Is Money?](#)

altcoins, [Altcoins: Currencies for Everyone](#), [Accelerating Innovation](#), [Currency as a Language](#), [Inventing Currency on the Playground](#), [Currency as an App](#)

value, [Authority by Production](#), [Valuing Currencies by Use](#)

an abstraction, [Characteristics of Money](#) animals use of, [How Old Is Money?](#), [Primates and Money](#) architecture, [Peer-to-Peer Architecture](#), [Master-Slave Architecture](#), [Negative Outcomes by Design, Not Intent](#) as a language, [Currency as a Means of Expression](#) as a liberator, [Banking: Liberator to Limiter](#) as an application, [Currency as an App](#) as emoji, [Transmitting Bitcoin Transactions via Skype as Smileys](#) asking permission, [New Architecture, New Access](#) ATM, [ATM Experience](#) atomic physics, [Bitcoin's Atomic Structure](#) authority, [Authority by Production](#), [Authority by Merit](#) authorization, [Bitcoin Transactions: Secure by Design](#) automobiles, [The Dangers of Automobiles, Electricity, and Bitcoin](#), [New Technologies, Riding on Old Infrastructure](#), [Interstitial Innovation](#)

B

backed by gold, [Just Another Abstraction of Money](#)

banking, [New Architecture, New Access](#), [Banks for Everyone](#), [Incumbent Reactions to Innovation](#), [Open Innovation and Opt-In Systems](#), [Including 6.5 Billion People in a Global Economy](#), [Bitcoin's Dumb Network](#), [Festival of the Commons](#), [From Banking to Bitcoin](#), [The Illusion of Senders, Receivers, and Accounts](#), [Banking Privilege and Surveillance](#)

as a liberator, [Banking: Liberator to Limiter](#)
inclusion, [Money of the People](#)
neutral network, [Net Neutrality and Non-Discrimination](#)
the experience, [Kids Use Bitcoin](#)
unbank, [Predicting the Future](#)
barter, [Technological Evolution of Money](#), [Characteristics of Money](#)bitcoin,
[Scaling is a Moving Target](#)breach, [Credit Cards: Insecure by Design](#)byob (be
your own bank), [Including 6.5 Billion People in a Global Economy](#)

C

cameras, [Incumbent Reactions to Innovation](#)
cat videos, [Cat Videos Will Destroy the Internet](#)
censorship, [Stopping Bitcoin Transactions Is Impossible](#)
censorship resistant, [Network-Centric Money Is Censorship Resistant](#)
characteristics of, [Barter to Precious Metals](#), [Characteristics of Money](#)
chemistry, [Bitcoin's Atomic Structure](#)
chemistry of, [Elements of Trust: Unleashing Creativity](#)
choice, [Born into Currency](#)
client-server architecture, [Client-Server Architecture](#)
closed network, [Open Innovation and Opt-In Systems](#)
comfort noise generation, [From Voice to Data](#)
commons
festival, [Festival of the Commons](#)
tragedy, [Tragedy of the Commons](#)
communicating value, [Technological Evolution of Money](#)communication, [How](#)
[Old Is Money?](#), [Communications Expanding While Access to Banking Is](#)
[Declining](#)community, [Bitcoin, the Zombie of Currencies](#), [Accelerating](#)
[Innovation](#), [Choosing Currencies and Communities](#)competition, [Festival of the](#)
[Commons](#), [Accelerating Innovation](#), [Infrastructure for Human Voices](#)consensus,
[Bitcoin, the Invention](#), [Dumb Networks, Innovation, and the Festival of the](#)

[Commons](#)content, [Money is the Message, Now Freed from the Medium](#)content type, [Money as a Content Type](#)cost of production, [Separating the Medium and the Message](#)creation, [Currency as a Means of Expression](#)creativity, [Building Blocks of Lego](#)credit cards, [Paper to Plastic](#), [Credit Cards: Insecure by Design](#)crime, [How Old Is Money?](#), [Bitcoin, the Zombie of Currencies](#), [The Dangers of Automobiles, Electricity, and Bitcoin](#), [Primates and Money](#)criticism, [The Dangers of Automobiles, Electricity, and Bitcoin](#)criticisms, [Infrastructure for Horses](#), [Infrastructure for Natural Gas](#)crowdfunding, [Building Blocks of Bitcoin](#)cultural hallucination, [Characteristics of Money](#)currency, [Valuing Currencies by Use](#)

choice, [Born into Currency](#)

community, [Choosing Currencies and Communities](#)

creation, [Currency as a Means of Expression](#)

evolution, [Currencies Evolve](#)

expression, [Currency as a Means of Expression](#)

index, [Index Currency](#)

paradigm, [Born into Currency](#)

sovereignty, [Currency Creates Sovereignty](#)

value, [Valuing Currencies by Use](#)

zero-sum game, [Born into Currency](#)

Currency

as an application, [Currency as an App](#)

meta-politics, [Choosing Currencies and Communities](#)

D

data, [From Voice to Data](#)

decentralization, [Communications Expanding While Access to Banking Is Declining](#), [New Architecture, New Access](#), [Network-Centric Money](#)

decentralized, [Open Innovation and Opt-In Systems](#)

design, [Negative Outcomes by Design, Not Intent](#), [Smart vs. Dumb Networks](#)

disruptive tech, [Designing for Innovation](#)

metaphors, [Bitcoin and Design](#)

purpose, [ATM Experience](#)

skeuomorphic, [Skeuomorphic Design](#)

user experience, [Bitcoin ATM Experience](#)

disruptarian, [Banking: Liberator to Limiter](#) disruptive tech, [Designing for Innovation](#) dumb, [Smart vs. Dumb Networks](#)

E

economic activities, [Primates and Money](#)

economic inclusion, [Communications Expanding While Access to Banking Is Declining](#)

economics, [Tragedy of the Commons](#)

electricity, [Infrastructure for Natural Gas](#), [From Natural Gas to Electricity](#)

elements, [Bitcoin's Atomic Structure](#)

email, [Multiple Currencies Coexist](#), [Alt Groups Will Destroy the Internet](#)

email attachments, [Email and Email Attachments Will Destroy the Internet](#)

Ether, [Choosing Currencies and Communities](#)

ethereum, [Currency as a Language](#)

evolution, [Currencies Evolve](#)

expression, [Currency as a Means of Expression](#)

F

fees, [Bitcoin, the Invention](#), [There Are No Spam Transactions in Bitcoin](#), [Open Innovation and Opt-In Systems](#), [Fee Optimization and Scaling](#), [Spam Transactions](#), [Legitimate Transactions](#), [Illegitimate Transactions](#)

festival, [Festival of the Commons](#)

festival of the commons, [Dumb Networks, Innovation, and the Festival of the Commons](#)

financial exclusion, [Dreaming of Totalitarian Control over All Financial Transactions](#)

financial inclusion, [Predicting the Future](#)

for consumers, [Open Innovation and Opt-In Systems](#)

freedom, [Communications Expanding While Access to Banking Is Declining](#),
[Censorship of Financial Transactions](#), [Bitcoin, the Zombie of Currencies](#),
[Banking Privilege and Surveillance](#)

G

game theory, [Open Innovation and Opt-In Systems](#)

geopolitics, [Communications Expanding While Access to Banking Is Declining](#)

global, [Money of the People](#), [Solving Payment Problems](#)

global culture, [Communications Expanding While Access to Banking Is Declining](#)

grand arc, [Grand Arc of Technology](#)

H

HD wallets, [Festival of the Commons 2012-2014](#)

hierarchy, [Banking: Liberator to Limiter](#)

honeypot, [Attacks Build Resistance](#)

I

identity, [Dreaming of Totalitarian Control over All Financial Transactions](#),
[Banking Privilege and Surveillance](#)

incentives, [Open Innovation and Opt-In Systems](#)

inclusion, [Money of the People](#), [Banks for Everyone](#), [Including 6.5 Billion People in a Global Economy](#), [Banking Privilege and Surveillance](#)

incremental tech, [Designing for Innovation](#)

index, [Index Currency](#)

infrastructure inversion, [Infrastructure Inversion](#), [From Horses to Vehicles](#)

banking, [From Banking to Bitcoin](#)

data, [From Voice to Data](#)

electricity, [From Natural Gas to Electricity](#)
paved roads, [From Horses to Vehicles](#)
innovation, [Recognizing Innovation](#), [Open Innovation and Opt-In Systems](#)
adoption, [Infrastructure for Natural Gas](#)
asking permission, [New Architecture, New Access](#)
automobiles, [The Dangers of Automobiles, Electricity, and Bitcoin](#), [New Technologies, Riding on Old Infrastructure](#)
banking, [New Architecture, New Access](#), [Open Innovation and Opt-In Systems](#), [Festival of the Commons](#), [Banking Privilege and Surveillance](#)
byob (be your own bank), [Including 6.5 Billion People in a Global Economy](#)
cameras, [Incumbent Reactions to Innovation](#)
competition, [Infrastructure for Human Voices](#)
creativity, [Building Blocks of Lego](#)
credit cards, [Paper to Plastic](#)
crime, [The Dangers of Automobiles, Electricity, and Bitcoin](#)
criticism, [The Dangers of Automobiles, Electricity, and Bitcoin](#)
criticisms, [Infrastructure for Horses](#), [Infrastructure for Natural Gas](#)
disruptive tech, [Designing for Innovation](#)
economic activities, [Primates and Money](#)
electricity, [Infrastructure for Natural Gas](#)
for consumers, [Open Innovation and Opt-In Systems](#)
HD wallets, [Festival of the Commons 2012-2014](#)
incremental tech, [Designing for Innovation](#)
infrastructure inversion, [From Horses to Vehicles](#)
internet, [UX and Society](#)
interstitial, [Interstitial Innovation](#)
investment, [Festival of the Commons 2012-2014](#)
Linux, [Incumbent Reactions to Innovation](#)

makers, [Recognizing Innovation](#)
mash-up, [Interstitial Innovation](#)
media, [Infrastructure for Natural Gas](#)
modem, [Infrastructure for Human Voices](#)
MP3, [Incumbent Reactions to Innovation](#)
multisignature, [Festival of the Commons 2012-2014](#)
new medium, [Separating the Medium and the Message](#)
open, [Incumbent Reactions to Innovation](#)
paper money, [Precious Metals to Paper](#)
permission, [The Smart Network - Phones](#)
permissionless, [Neutrality, Criminals, and Bitcoin](#), [New Architecture](#), [New Access](#), [Bitcoin's Dumb Network](#)
regulation, [Predicting the Future](#)
tools for, [Building Blocks of Creativity](#)
wallet, [Fee Optimization and Scaling](#)
international finance, [Money of the People](#)internet, [Bitcoin, the Invention](#),
[Neutrality, Criminals, and Bitcoin](#), [New Architecture](#), [New Access](#), [The Dumb Network - Internet](#), [UX and Society](#), [Usenet Will Destroy the Internet](#)
printing press, [Authority by Production](#)
interstitial, [Interstitial Innovation](#)investment, [Festival of the Commons 2012-2014](#)

K

keys, [Master-Slave Architecture](#), [Wallets aren't wallets](#)
permission, [Wallets aren't wallets](#)

L

language, [How Old Is Money?](#)
lightning network, [Building Blocks of Bitcoin](#)
Linux, [Incumbent Reactions to Innovation](#)

Litecoin, [Choosing Currencies and Communities](#)

M

makers, [Recognizing Innovation](#)

mash-up, [Interstitial Innovation](#)

master-slave architecture, [Master-Slave Architecture](#)

media, [Infrastructure for Natural Gas](#)

medium

message, [Separating the Medium and the Message](#)

message, [Separating the Medium and the Message](#)meta-currencies, [Index](#)

[Currency](#)meta-instrument, [Index Currency](#)meta-politics, [Choosing Currencies](#)

[and Communities](#)metaphors, [Bitcoin and Design](#)micropayments, [Solving](#)

[Payment Problems](#)microtransactions, [Solving Payment Problems](#)modem,

[Infrastructure for Human Voices](#)money, [Born into Currency](#), [Valuing Currencies by Use](#)

abstract value, [Barter to Precious Metals](#)

age of, [How Old Is Money?](#)

an abstraction, [Characteristics of Money](#)

animals use of, [How Old Is Money?](#), [Primates and Money](#)

architecture, [Master-Slave Architecture](#)

as a language, [Currency as a Means of Expression](#)

backed by gold, [Just Another Abstraction of Money](#)

characteristics of, [Barter to Precious Metals](#), [Characteristics of Money](#)

chemistry of, [Elements of Trust: Unleashing Creativity](#)

communicating value, [Technological Evolution of Money](#)

communication, [How Old Is Money?](#)

content type, [Money as a Content Type](#)

cultural hallucination, [Characteristics of Money](#)

language, [How Old Is Money?](#)

network-centric, [Network-Centric Money](#)
precious metals, [Barter to Precious Metals](#)
protocol, [Moving to a Network-Centric, Protocol-Based Era](#)
taboo, [Client-Server Architecture](#)
technology of, [Bitcoin Design Principles](#)
value of, [Characteristics of Money](#)
MP3, [Incumbent Reactions to Innovation](#)multisignature, [Festival of the Commons 2012-2014](#), [Building Blocks of Bitcoin](#)

N

netflix, [Netflix Will Destroy the Internet](#)
network, [Alt Groups Will Destroy the Internet](#)
architecture, [Peer-to-Peer Architecture](#)
client-server architecture, [Client-Server Architecture](#)
closed network, [Open Innovation and Opt-In Systems](#)
dumb, [Smart vs. Dumb Networks](#)
master-slave architecture, [Master-Slave Architecture](#)
payment, [Money is the Message, Now Freed from the Medium](#)
smart, [The Smart Network - Phones](#)
network-centric, [Network-Centric Money](#)network-centric era, [Moving to a Network-Centric, Protocol-Based Era](#)neutral network, [Net Neutrality and Non-Discrimination](#)neutrality, [New Architecture, New Access](#), [Net Neutrality and Non-Discrimination](#), [Network-Centric Money Is Censorship Resistant](#), [Bitcoin's Dumb Network](#), [Spam Transactions, Legitimate Transactions, Illegitimate Transactions](#)new medium, [Separating the Medium and the Message](#)

O

open, [Incumbent Reactions to Innovation](#)

P

panopticon, [Sousveillance, Not Surveillance](#)

paper money, [Precious Metals to Paper](#)
paradigm, [Born into Currency](#)
paved roads, [From Horses to Vehicles](#)
payment, [Money is the Message, Now Freed from the Medium](#)
global, [Money of the People](#), [Solving Payment Problems](#)
payment channels, [Building Blocks of Bitcoin](#)payment systems,
[Communications Expanding While Access to Banking Is Declining](#)permission,
[The Smart Network - Phones, Wallets aren't wallets](#)permissioned, [Bitcoin's Dumb Network](#)permissionless, [Neutrality, Criminals, and Bitcoin](#), [New Architecture, New Access, Bitcoin's Dumb Network](#)precious metals, [Barter to Precious Metals](#)printing press, [Authority by Production](#)privacy, [Censorship of Financial Transactions](#), [Sousveillance, Not Surveillance](#), [Banks for Everyone](#)privacy vs. secrecy, [Sousveillance, Not Surveillance](#)production cost, [Money is the Message, Now Freed from the Medium](#)protocol, [Moving to a Network-Centric, Protocol-Based Era](#)publishing, [Authority by Production](#)purpose, [ATM Experience](#)

R

receiver, [The Illusion of Senders, Receivers, and Accounts](#)
recipe, [Building Blocks of Cooking](#)
regulation, [The Dangers of Automobiles, Electricity, and Bitcoin](#), [Predicting the Future](#)
remittances, [Money of the People](#), [Including 6.5 Billion People in a Global Economy](#), [Remittances, Impacting Lives around the World](#), [Interstitial Innovation](#)

S

scaling, [Attacks Build Resistance](#)
bitcoin, [Scaling is a Moving Target](#)
cat videos, [Cat Videos Will Destroy the Internet](#)
email, [Alt Groups Will Destroy the Internet](#)
email attachments, [Email and Email Attachments Will Destroy the Internet](#)

netflix, [Netflix Will Destroy the Internet](#)
the alt, [Alt Groups Will Destroy the Internet](#)
usenet, [Usenet Will Destroy the Internet](#)
VOIP, [VOIP Will Destroy the Internet](#)
secrecy, [Sousveillance, Not Surveillance](#)security, [Master-Slave Architecture](#),
[Attacks Build Resistance](#), [Open Innovation and Opt-In Systems](#), [Money as a Content Type](#)
authorization, [Bitcoin Transactions: Secure by Design](#)
breach, [Credit Cards: Insecure by Design](#)
credit cards, [Credit Cards: Insecure by Design](#)
self-owning cars
automobiles, [Interstitial Innovation](#)
sender, [The Illusion of Senders, Receivers, and Accounts](#)settlement, [Fee Optimization and Scalings](#)short wave radio, [Transmitting Bitcoin Transactions via Short Wave Radios](#)skeuomorphic, [Skeuomorphic Design](#)smart, [The Smart Network - Phones](#)source code, [The Illusion of Senders, Receivers, and Accounts](#)sousveillance, [Sousveillance, Not Surveillance](#)sovereignty, [Currency Creates Sovereignty](#)spam, [There Are No Spam Transactions in Bitcoin](#), [Alt Groups Will Destroy the Internet](#), [Fee Optimization and Scaling](#), [Spam Transactions, Legitimate Transactions, Illegitimate Transactions](#)surveillance, [Dreaming of Totalitarian Control over All Financial Transactions](#), [Censorship of Financial Transactions](#), [Sousveillance, Not Surveillance](#), [Banking Privilege and Surveillance](#)systems
architecture, [Negative Outcomes by Design, Not Intent](#)

T

taboo, [Client-Server Architecture](#)
technology
grand arc, [Grand Arc of Technology](#)
technology of, [Bitcoin Design Principle](#)telephone, [Infrastructure for Human Voices](#), [From Voice to Data](#)the alt, [Alt Groups Will Destroy the Internet](#)the experience, [Kids Use Bitcoin](#)time lock, [Building Blocks of Bitcoin](#)tools for, [Building Blocks of Creativity](#)tragedy, [Tragedy of the Common](#)transaction,

Money as a Content Type

fees, [Bitcoin, the Invention](#), [There Are No Spam Transactions in Bitcoin](#), [Open Innovation and Opt-In Systems](#)

multisignature, [Building Blocks of Bitcoin](#)

time lock, [Building Blocks of Bitcoin](#)

transactions, [Fee Optimization and Scaling](#)

as emoji, [Transmitting Bitcoin Transactions via Skype as Smileys](#)

microtransactions, [Solving Payment Problems](#)

short wave radio, [Transmitting Bitcoin Transactions via Short Wave Radio](#)

transparency, [Sousveillance, Not Surveillance](#)trust, [Network-Centric Money](#), [Bitcoin's Atomic Structure](#)trust platform, [Bitcoin's Atomic Structure](#)

U

unbank, [Predicting the Future](#)

usenet, [Usenet Will Destroy the Internet](#)

user experience, [Bitcoin ATM Experience](#), [Brand New Tech, Same Old Terms](#)

V

value, [Authority by Production](#), [Valuing Currencies by Use](#)

value of, [Characteristics of Money](#)

value of content

cost of production, [Separating the Medium and the Message](#)

value to consumer, [Separating the Medium and the Message](#)

value to consumer, [Separating the Medium and the Message](#)VOIP, [VOIP Will Destroy the Internet](#)

W

wallet, [Wallets aren't wallets](#), [Bitcoin's Atomic Structure](#), [Fee Optimization and Scaling](#)

wire transfer, [The Joys of International Wire Transfer](#)

Z

zero-sum game, [Born into Currency](#)



See our research on: [Russia](#) | [Supreme Court](#) | [COVID-19](#)



Pew Research Center

Search [pewresearch.org...](#)



RESEARCH TOPICS ▼ ALL PUBLICATIONS METHODS SHORT READS TOOLS & RESOURCES EXPERTS ABO

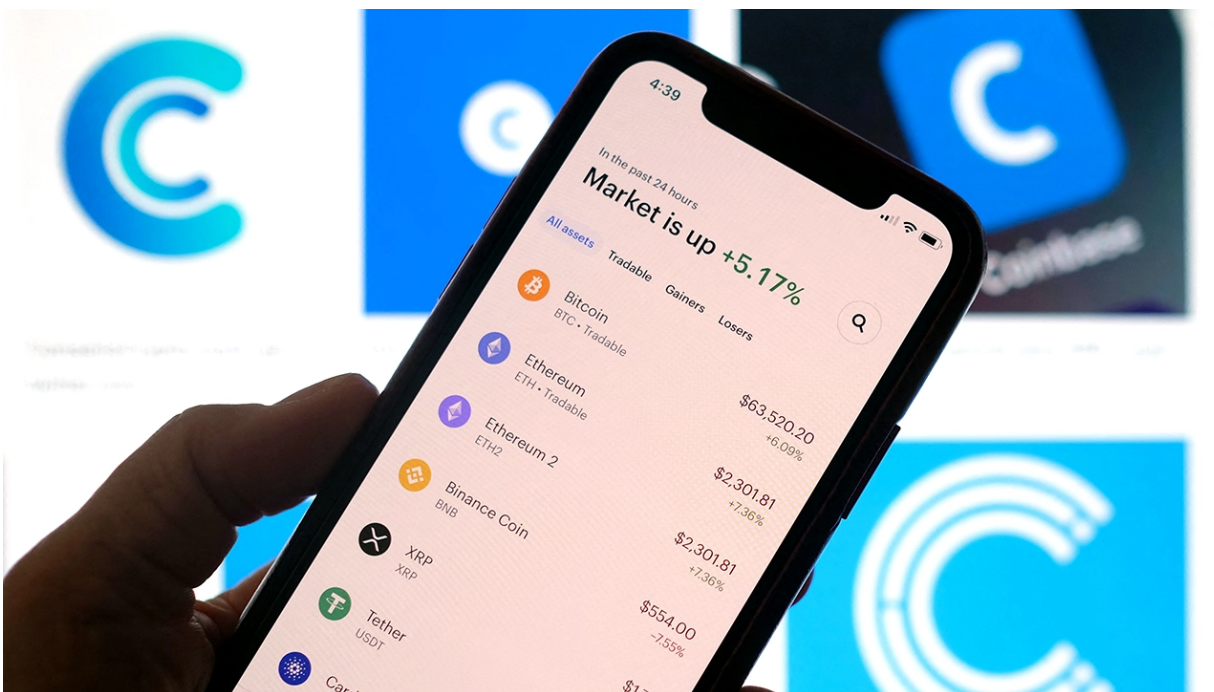
[Home](#) > [Research Topics](#) > [Internet & Technology](#) > [Emerging Technology](#)

NOVEMBER 11, 2021



16% of Americans say they have ever invested in, traded or used cryptocurrency

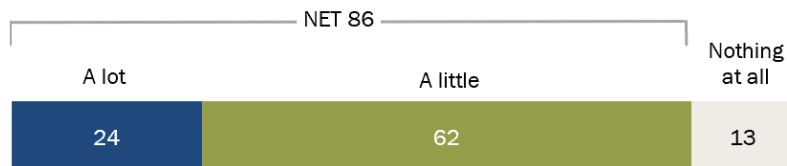
BY ANDREW PERRIN



The vast majority of U.S. adults have heard at least a little about cryptocurrencies like Bitcoin or Ether, and 16% say they personally have invested in, traded or otherwise used one, according to a new Pew Research Center survey. Men ages 18 to 29 are particularly likely to say they have used cryptocurrencies.

Nearly nine-in-ten Americans say they have heard at least a little about cryptocurrency ...

% of U.S. adults who say they have heard ____, if anything, about cryptocurrency such as Bitcoin or Ether



... and 16% say they have ever invested in, traded or used one themselves

% of U.S. adults who say they themselves __ ever invested in, traded or used a cryptocurrency such as Bitcoin or Ether



Note: The 14% of U.S. adults who said they had heard nothing at all about cryptocurrency, or gave no answer, did not receive the question about investing in, trading or using a cryptocurrency. Those who did not give an answer are not shown.

Source: Survey of U.S. adults conducted Sept. 13-19, 2021.

PEW RESEARCH CENTER

Overall, 86% of Americans say they have heard at least a little about cryptocurrencies, including 24% who say they have heard a lot about them, according to the survey of U.S. adults, conducted Sept. 13-19, 2021. Some 13% say they have heard nothing at all.

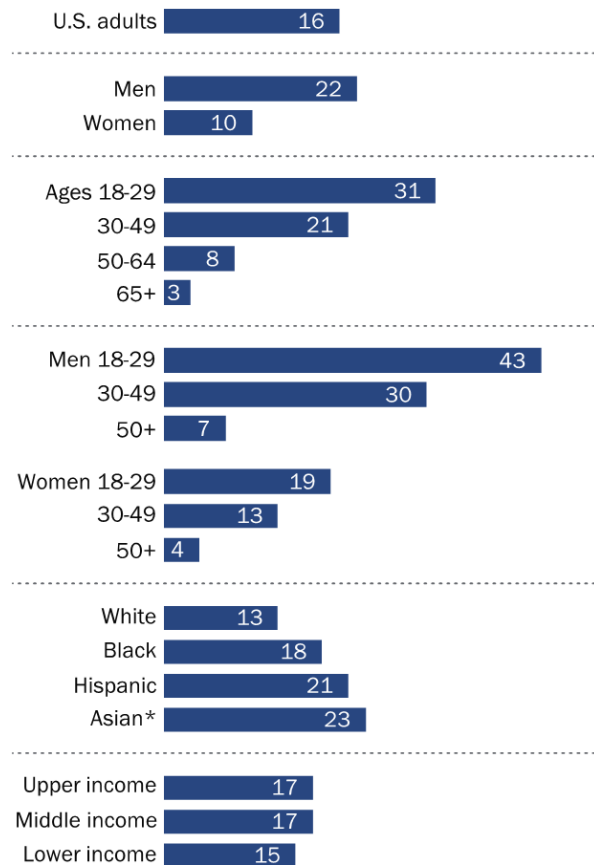
In 2015, the Center asked Americans [different questions](#) that were focused exclusively on Bitcoin. At the time, 48% of adults said they had heard of Bitcoin (to any degree), and just 1% said they had ever collected, traded or used it.

How we did this ⊕

In the new survey, certain demographic groups are particularly likely to say they have used cryptocurrencies, with some of the largest differences by age and gender.

43% of men ages 18 to 29 say they have invested in, traded or used a cryptocurrency

% of U.S. adults who say they themselves have ever invested in, traded or used a cryptocurrency such as Bitcoin or Ether



*Asian adults were interviewed in English only.

Note: Family income tiers are based on adjusted 2020 earnings.

White, Black and Asian adults include those who report being only one race and are not Hispanic. Hispanics are of any race. Those who did not give an answer are not shown.

Source: Survey of U.S. adults conducted Sept. 13-19, 2021.

PEW RESEARCH CENTER

Roughly three-in-ten Americans ages 18 to 29 (31%) say they have ever invested in, traded or used a cryptocurrency such as Bitcoin or Ether, compared with smaller shares of adults in older age groups. Men are about twice as likely as women to say they ever used a cryptocurrency (22% vs. 10%).

These differences are especially pronounced when looking at age and gender together. About four-in-ten men ages 18 to 29 (43%), for example, say they have ever invested in, traded or used a cryptocurrency, compared with 19% of women in the same age range. Among both men and women, the likelihood of having invested in, traded or used cryptocurrency decreases with age.

Asian, Black and Hispanic adults are more likely than White adults to say they have ever invested in, traded or used a cryptocurrency. There are no statistically significant differences by household income.

While majorities across demographic groups say they have heard at least a little about cryptocurrency, smaller shares say they have heard a lot. For example, adults under 50 (31%) and men (35%) are more likely than older Americans (16%) and women (15%), respectively, to say they have heard a lot.

The share of adults who have heard a lot about cryptocurrency also varies by race, ethnicity and household income. For example, 43% of Asian Americans say they have heard a lot about cryptocurrency, compared with 29% of Hispanic adults and about a quarter of Black or White adults. Americans with higher incomes (31%) are more likely than those with middle (25%) and lower incomes (21%) to have heard a lot about cryptocurrency.

These findings emerge as government leaders and others [debate the regulation](#) of cryptocurrency – which [has been defined](#) as a medium of exchange that is digital, encrypted and decentralized, with no central authority that manages and maintains its value. Financial regulators have worried about [policing cryptocurrencies](#) and have raised concerns about the [long-term viability](#) of such currencies, such as Bitcoin.

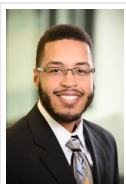
China recently [banned transactions using cryptocurrencies](#). U.S. Federal Reserve Board Chairman Jerome Powell said this summer that these currencies [need more regulation](#), and the Biden administration is trying to [combat ransomware](#) by cracking down on cryptocurrency payments. At the same time, El Salvador in September became the first country [to declare Bitcoin](#) as legal tender.

Note: Here are [the questions used for this report, along with responses, and its methodology](#).

Topics [Personal Finances](#), [Technology Adoption](#), [Emerging Technology](#)

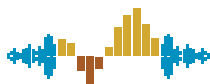
SHARE THIS LINK:

<https://pewrsr.ch/3quL14Y>



Andrew Perrin is a research analyst focusing on internet and technology at Pew Research Center.

[POSTS](#) | [BIO](#) | [EMAIL](#)



Add Pew Research Center to your Alexa

Say "Alexa, enable the Pew Research Center flash briefing"

[ADD TO ALEXA](#)

RELATED

SHORT READ | OCT 7, 2021

Two-thirds of U.S. Catholics unaware of pope's new restrictions on traditional Latin Mass

SHORT READ | OCT 18, 2019

Most U.S. adults intend to participate in 2020 census, but some demographic groups aren't sure

SHORT READ | SEP 16, 2020

Americans have heard more about clashes between police and protesters than other recent news stories

SHORT READ | NOV 16, 2020

5 facts about the QAnon conspiracy theories

SHORT READ | JUN 11, 2021

U.S. adults have mixed views on whether geoengineering would help reduce effects of climate change

TOPICS

Emerging Technology

Personal Finances

Technology Adoption

MOST POPULAR

SHORT READ | MAR 9, 2022

Majority of workers who quit a job in 2021 cite low pay, no opportunities for advancement, feeling disrespected

FEATURE | NOV 9, 2021

Political Typology Quiz

SHORT READ | JAN 17, 2019

Where Millennials end and Generation Z begins

REPORT | JAN 9, 2020

Trends in income and wealth inequality

SHORT READ | DEC 9, 2021

Gasoline costs more these days, but price spikes have a long history and happen for a host of reasons







Pew Research Center 

1615 L St. NW, Suite 800
Washington, DC 20036
USA
(+1) 202-419-4300 | Main
(+1) 202-857-8562 | Fax
[\(+1\) 202-419-4372 | Media
Inquiries](#)

RESEARCH TOPICS

- Politics & Policy
- International Affairs
- Immigration & Migration
- Race & Ethnicity
- Religion
- Generations & Age
- Gender & LGBT
- Family & Relationships
- Economy & Work
- Science
- Internet & Technology
- News Habits & Media
- Methodological Research
- [Full topic list](#)

FOLLOW US

-  Email Newsletters
-  Facebook
-  Twitter
-  Tumblr
-  YouTube
-  RSS

ABOUT PEW RESEARCH CENTER Pew Research Center is a nonpartisan fact tank that informs the public about the issues, attitudes and trends shaping the world. It conducts public opinion polling, demographic research, media content analysis and other empirical social science research. Pew Research Center does not take policy positions. It is a subsidiary of [The Pew Charitable Trusts](#).

CBO

Trends in the Internal Revenue Service's Funding and Enforcement



© Natalia Bratslavsky/Shutterstock.com

JULY 2020

At a Glance

The Internal Revenue Service (IRS) promotes compliance with tax laws in many ways: It verifies information provided by taxpayers, works to prevent the distribution of refunds that are claimed erroneously, audits tax returns, and attempts to collect unpaid taxes and unfiled returns, among other efforts. In this report, the Congressional Budget Office examines how those activities declined over the 2010–2018 period as the service’s resources decreased and how changes to the IRS’s budget could affect federal revenues.

- In its most recent report on uncollected taxes, the IRS estimated that an average of \$441 billion (16 percent) of the taxes owed annually between 2011 and 2013 was not paid in accordance with the law. Most of the unpaid taxes were the result of taxpayers’ underreporting their income. Through enforcement, the IRS collected an average of \$60 billion of those unpaid taxes annually, reducing the gap between taxes owed and taxes paid in those years to \$381 billion per year, on average.
- The IRS’s appropriations have fallen by 20 percent in inflation-adjusted dollars since 2010, resulting in the elimination of 22 percent of its staff. The amount of funding and staff allocated to enforcement activities has declined by about 30 percent since 2010.
- Since 2010, the IRS has done less to enforce tax laws. Between 2010 and 2018, the share of individual income tax returns it examined fell by 46 percent, and the share of corporate income tax returns it examined fell by 37 percent. The disruptions stemming from the 2020 coronavirus pandemic will further reduce the ability of the IRS to enforce tax laws.
- CBO estimates that increasing the IRS’s funding for examinations and collections by \$20 billion over 10 years would increase revenues by \$61 billion and that increasing such funding by \$40 billion over 10 years would increase revenues by \$103 billion.
- CBO’s estimates are subject to considerable uncertainty and only capture the direct effect of enforcement activities. The IRS’s enforcement activities have an indirect effect on the tax gap by discouraging taxpayers from making misstatements on their returns.



Contents

Summary	1
How Much Tax Goes Uncollected Each Year?	1
How Does the Internal Revenue Service Enforce Tax Laws?	1
How Has Funding for the Internal Revenue Service Changed Over Time?	1
How Have Reductions in Funding and Staffing Affected Enforcement?	2
How Might an Increase in Funding for Enforcement Affect Federal Tax Receipts?	2
The Gap Between the Amount of Taxes Owed and the Amount Paid	2
Components of the Tax Gap	3
Factors That Affect the Size of the Tax Gap	4
How the Internal Revenue Service Enforces Tax Laws	7
Preliminary Screening and Assessment	7
Comparison of Returns With Information From Third Parties	7
Examinations	7
Collections	8
Employees' Role	8
Indirect Effects of Enforcement	8
Trends in Funding and Staffing	8
Recent Appropriations	8
BOX 1. DETERRENT EFFECTS OF ENFORCEMENT	9
Appropriations From 2010 to 2018	10
Staffing	11
Trends in Enforcement	11
Examinations of Individual Income Tax Returns	11
Examinations of Corporate Income Tax Returns	12
Additional Taxes Recommended Following Examinations	13
Appeals of Recommended Additional Taxes and Penalties	13
BOX 2. IMPROPER PAYMENTS AND THE EARNED INCOME TAX CREDIT	14
Automated Enforcement Activity	15
Collections Revenues	15
Collections Activity	16
Impact of the Coronavirus Pandemic on Enforcement	17

How Changes in Funding Would Affect Future Revenues	18
Estimated Effect on Revenues of Two Options to Increase Funding	19
Scorekeeping Guidelines for Formal Cost Estimates	21
How Enforcement Spending Is Reflected in Baseline Revenue Projections	21
BOX 3. OPTIONS FOR INCREASING TAX REVENUES	22
Sources of Uncertainty	22
Appendix A: Detailed View of Tax Law Enforcement	25
Appendix B: CBO’s Approach to Estimating Changes in Revenues	31
List of Tables and Figures	33
About This Document	34

Notes

The *Internal Revenue Service Data Book, 2019* was released on June 30, 2020. Because the date of that release did not allow enough time for the Congressional Budget Office to incorporate those data in its analysis, this report is based on data from the *Internal Revenue Service Data Book, 2018* and earlier years.

Unless this report indicates otherwise, all years referred to are federal fiscal years, which run from October 1 through September 30 and are designated by the calendar year in which they end.

Numbers in the text, tables, and figures may not add up to totals because of rounding.

To remove the effects of inflation, CBO adjusted discretionary funding related to federal personnel with the employment cost index for wages and salaries and expressed those amounts in 2018 dollars; other types of discretionary funding were adjusted with the gross domestic product price index and expressed in 2018 dollars. Dollar amounts other than discretionary funding were adjusted with the personal consumption expenditure index and expressed in 2018 dollars. Estimates of the tax gap and the estimated revenue effects of changes to funding for the Internal Revenue Service are in nominal (current) dollars.



Trends in the Internal Revenue Service's Funding and Enforcement

Summary

The Internal Revenue Service (IRS) collected \$3.5 trillion in taxes in 2018, nearly 95 percent of total federal revenues. To do so, it relied largely on taxpayers to report their income, calculate the amount of tax they owed, and remit that amount to the IRS through withholding or other payments. However, some taxpayers have failed to pay hundreds of billions of dollars in taxes, the IRS estimates. Policymakers have expressed interest in how changes in IRS funding, particularly for enforcement of tax laws, could increase the federal government's tax revenues.

This report describes how the IRS encourages and enforces compliance with tax laws. It examines the IRS's enforcement activities between 2010 and 2018 and analyzes how the decline in those activities reflects the decline in its funding and staff over that period. On the basis of the relationship between enforcement funding and revenues, the Congressional Budget Office estimates the effects an increase in IRS funding for enforcement could have on federal tax receipts.

How Much Tax Goes Uncollected Each Year?

The difference between the amount of taxes owed and the amount collected each year—often called the tax gap—is estimated periodically by the IRS. The *gross* tax gap is the amount that taxpayers do not pay by their filing deadline. As such, it measures the extent of non-compliance with the tax code. In its most recent report, the IRS estimated that the annual gross tax gap was \$441 billion, on average, between 2011 and 2013.

The IRS ultimately collects some of that amount. The *net* tax gap, which is the gross tax gap reduced by the amount that the IRS collects through its enforcement activities, was an estimated \$381 billion annually over that period. In addition, the IRS's enforcement activities have an indirect effect on the tax gap by discouraging taxpayers from making misstatements on their returns. The size of the tax gap is also affected by whether income is visible to the IRS and by the complexity of the tax code, among other factors.

How Does the Internal Revenue Service Enforce Tax Laws?

The IRS undertakes a variety of enforcement activities:

- Auditing tax returns,
- Collecting unpaid taxes,
- Obtaining tax returns from taxpayers who did not file returns on time,
- Correcting mathematical or clerical errors,
- Using software to flag questionable refunds, and
- Verifying information reported by taxpayers against information from third parties.

How Has Funding for the Internal Revenue Service Changed Over Time?

Appropriations for the IRS have fallen by a total of about 20 percent in real (inflation-adjusted) dollars between 2010 and 2018. With the exception of 2016, real appropriations have consistently fallen below the previous year's level over that period. Because labor costs account for about 70 percent of the IRS's budget, measures to reduce its workforce were instituted, including a hiring freeze. Those measures resulted in a 22 percent decline in the number of employees at the agency and a 30 percent decline in the number of employees working in enforcement roles.¹ The number of revenue agents and revenue officers, highly specialized enforcement employees who handle the most complex examinations and collections cases, fell by 35 percent and 48 percent, respectively, between 2010 and 2018.

1. Those figures are measured as a decline in the number of full-time equivalents (FTEs). Because not all employees work full time in a given year, the IRS calculates the number of FTEs as the total number of hours worked divided by the number of hours that a full-time employee would work.

How Have Reductions in Funding and Staffing Affected Enforcement?

As the IRS's budget and workforce declined, so did its examination rates for both individual and corporate income tax returns. (The examination rate is the number of examinations closed in a fiscal year divided by the number of returns filed in the previous calendar year.) The overall examination rate for all returns fell by about 40 percent between 2010 and 2018. Over that period:

- The examination rate for individual income tax returns dropped by about 46 percent. About 0.6 percent of individual income tax returns were examined in 2018.
- The examination rate for corporate income tax returns fell by about 37 percent. In 2018, 0.9 percent of corporate income tax returns were examined.
- Larger corporations were more likely to have their returns examined than smaller ones over the 2010–2018 period. However, the examination rates for large corporations—those with assets of more than \$10 million—declined more steeply between 2010 and 2018 than examination rates for corporations with fewer assets did.
- Similarly, higher-income individuals were more likely to be examined than lower-income ones over the period. However, the examination rate for higher-income taxpayers fell, while the examination rate for lower-income taxpayers remained fairly stable. Nearly all examinations of lower-income taxpayers were initiated because of claims for the earned income tax credit.
- The amount of additional taxes and penalties the IRS recommended after examinations of corporate and individual income tax returns—before taxpayers appeal or challenge those recommendations—also fell from 2010 to 2018. The decline occurred because the IRS closed fewer examinations each year.

The amount of delinquent tax debt, or unpaid assessments, increased from 2010 to 2018. The amount of revenue received from that debt as a result of collections activities, however, remained between 8 percent and 10 percent of unpaid assessments over the period. The number of delinquent taxpayer accounts, resulting

from returns filed without payment of all taxes due or examination assessments not paid promptly, generally increased from 2010 to 2018. The IRS is also responsible for securing returns that were not filed on time. The number of investigations of delinquent filers fell over the 2010–2018 period.

Trends are unlikely to reverse in the near future. The disruptions stemming from the 2020 coronavirus pandemic will reduce the IRS's enforcement activities and pose new challenges for taxpayers in complying with tax laws.

How Might an Increase in Funding for Enforcement Affect Federal Tax Receipts?

On the basis of its analysis of the effects that different funding levels have had on IRS enforcement, CBO estimates that increasing the IRS's funding for examinations and collections by \$20 billion over 10 years would boost revenues by \$61 billion, resulting in a \$41 billion decrease in the cumulative deficit; increasing such funding by \$40 billion over 10 years would boost revenues by \$103 billion, resulting in a \$63 billion decrease in the deficit.

CBO's estimates for those two options are uncertain and only capture the direct effect of enforcement activities. Any indirect benefits of increasing enforcement, such as deterring taxpayers from violating tax laws, are excluded from the estimates.

Because of the budget scorekeeping guidelines used by the Congress, only the spending increases attributable to those options would be counted in a cost estimate. However, if an appropriation bill or another bill providing funding for one of the options were enacted, CBO's next projection of the budget deficit would incorporate the estimated effects of the funding increase on tax revenues.

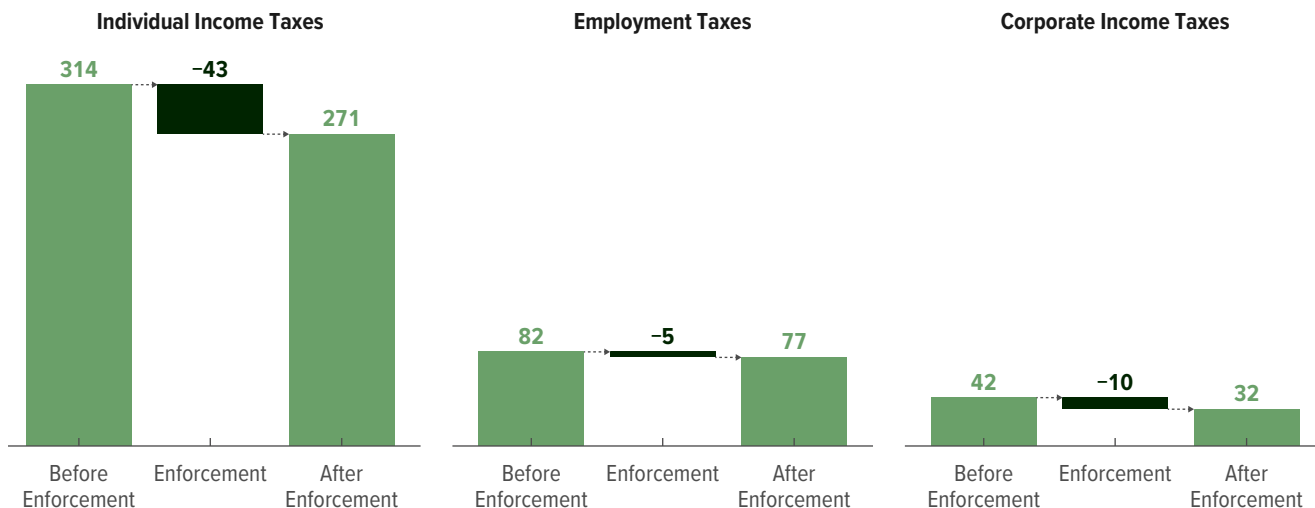
The Gap Between the Amount of Taxes Owed and the Amount Paid

Although the IRS collected, on average, about \$2.3 trillion in taxes annually between tax years 2011 and 2013, in its most recent report on the tax gap it estimated that taxpayers actually owed hundreds of billions of dollars more in those years. The IRS periodically estimates the tax gap using a variety of methods, including data from its examinations of tax returns, statistical models, and comparisons of the returns filed by taxpayers to external data or actual receipts.

Figure 1.

Estimated Amount of Unpaid Taxes

Billions of Dollars



Source: Congressional Budget Office, using data from the Internal Revenue Service.

The estimates are an annual average of the amount of taxes that were not paid over the 2011–2013 period.

Employment taxes include Social Security, Medicare, and federal unemployment taxes.

Estate, gift, and excise taxes, which together account for less than 1 percent of underreported taxes, are not shown.

The IRS estimated that the *gross* tax gap—the difference between the total amount of federal taxes that taxpayers owed and the amount that was paid on or before the filing deadline—averaged \$441 billion annually from 2011 to 2013 (see Figure 1). That figure was 2.7 percent of the nation's gross domestic product and about 16 percent of federal taxes owed.² The gap occurred because taxpayers underreported their liability (for example, by not reporting all sources of income or overstating deductions from income), failed to include full payment with their return, or failed to file a required return in any of five categories: individual income, corporate income, employment, estate and gift, and excise.

Whereas the gross tax gap measures the extent of non-compliance, the *net* tax gap reflects the ability of the IRS to enforce the law. The net tax gap—defined as the

amount of taxes that remains unpaid after the IRS has sought through administrative or enforcement actions to collect taxes owed—averaged \$381 billion annually between 2011 and 2013.³

Components of the Tax Gap

The IRS analyzes the ways that taxpayers avoid paying the full amount of taxes they owe so that the agency can determine where to direct its resources for enforcement. About 80 percent (\$352 billion) of the annual gross tax gap over the 2011–2013 period occurred because taxpayers underreported their liability (see Figure 2). They either understated their income or overstated tax credits, tax deductions, or income adjustments. The remainder of the gross tax gap was attributable to taxpayers who filed a return but did not pay their taxes in full (\$50 billion) and to taxpayers who failed to file a required return (\$39 billion).

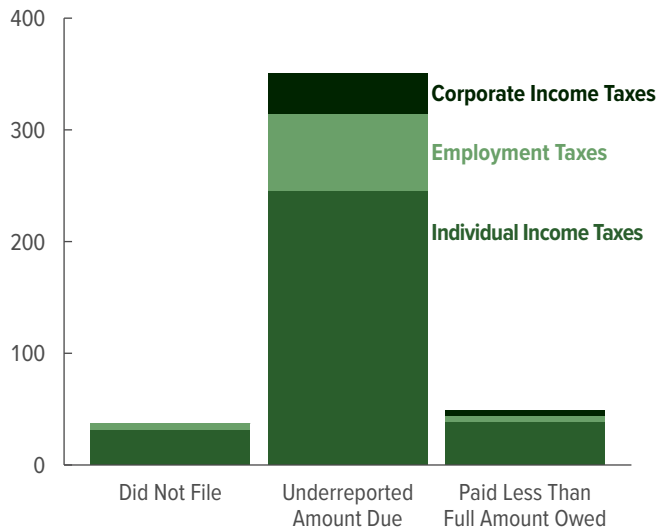
2. For details of how those estimates were created, see Internal Revenue Service, *Federal Tax Compliance Research: Tax Gap Estimates for Tax Years 2011–2013*, Publication 1415 (September 2019), www.irs.gov/pub/irs-pdf/p1415.pdf (1.4 MB). Those estimates are the most recent available.

3. Payments counted in measuring the net tax gap include both those obtained through enforcement actions and those made after the due date without the IRS's intervention. For example, a taxpayer might make a payment when filing an amended return.

Figure 2.

Unpaid Taxes, by Method of Avoiding Payment

Billions of Dollars



Source: Internal Revenue Service.

The estimates are an annual average of the amount of taxes that were not paid over the 2011–2013 period.

Employment taxes include Social Security, Medicare, and federal unemployment taxes.

Estate, gift, and excise taxes, which together account for less than 1 percent of underreported taxes, are not shown.

The IRS does not estimate how many corporations failed to file.

The largest amount of underreported liability (\$245 billion) occurred because individual taxpayers underreported their income (see Figure 3). Most of that underreported income was the result of underreported business income (\$110 billion), underreported non-business income (\$57 billion), or overstated credits (\$42 billion).⁴

The IRS reduced the tax gap from 2011 to 2013 by \$60 billion a year, on average, through administrative and enforcement actions. Of that \$60 billion, the tax agency collected an average of \$43 billion (72 percent) in individual income taxes and \$10 billion (17 percent) in corporate income taxes.

4. Business income includes nonfarm proprietor income; flow-through income from partnerships, S corporations, and estates and trusts that is taxed at the individual level; rent and royalty income; and farm income. Those forms of income are reported on Schedules C, E, and F. Nonbusiness income includes wages and salaries, interest, dividends, pensions and annuities, unemployment compensation, Social Security benefits, and capital gains.

Factors That Affect the Size of the Tax Gap

The IRS's ability to reduce the net tax gap through enforcement and other activities depends partly on its budget and staff, but other factors also have an effect: whether taxpayers' income is reported to the IRS by a third party, whether tax is withheld from payments to the taxpayers, the complexity of the tax code, and the availability of resources that can facilitate compliance, such as IRS publications or paid preparers with expertise.

Visibility of Income and Withholding. Some organizations inform both taxpayers and the IRS of payments to taxpayers, making that income visible to the IRS. For example, employers report wages and salaries on IRS Form W-2. Such third-party information reporting can increase voluntary compliance by minimizing taxpayers' recordkeeping burden and by making them less likely to underreport earnings. Reporting also allows the IRS to more easily verify amounts reported on a return. Items that are subject to substantial information reporting tend to be accurately reported on income tax returns.

In contrast, items that are subject to little or no third-party information reporting account for most of the underreported income (see Figure 4). For example, although the IRS receives information on some businesses' gross receipts, it does not receive independent information on expenses. Noncompliant taxpayers can, therefore, inflate their expenses to minimize their net profit from a business.⁵

In recent years, the scope of third-party information reporting has expanded. Payment settlement entities, such as banks and other processors of credit card transactions, are required to report certain payments to individuals on IRS Form 1099-K.⁶ When certain assets are sold, brokers and investment managers must include information on the original cost of the assets on IRS Form 1099-B, thus showing the amount of a transaction that is taxed as a capital gain. Some foreign financial

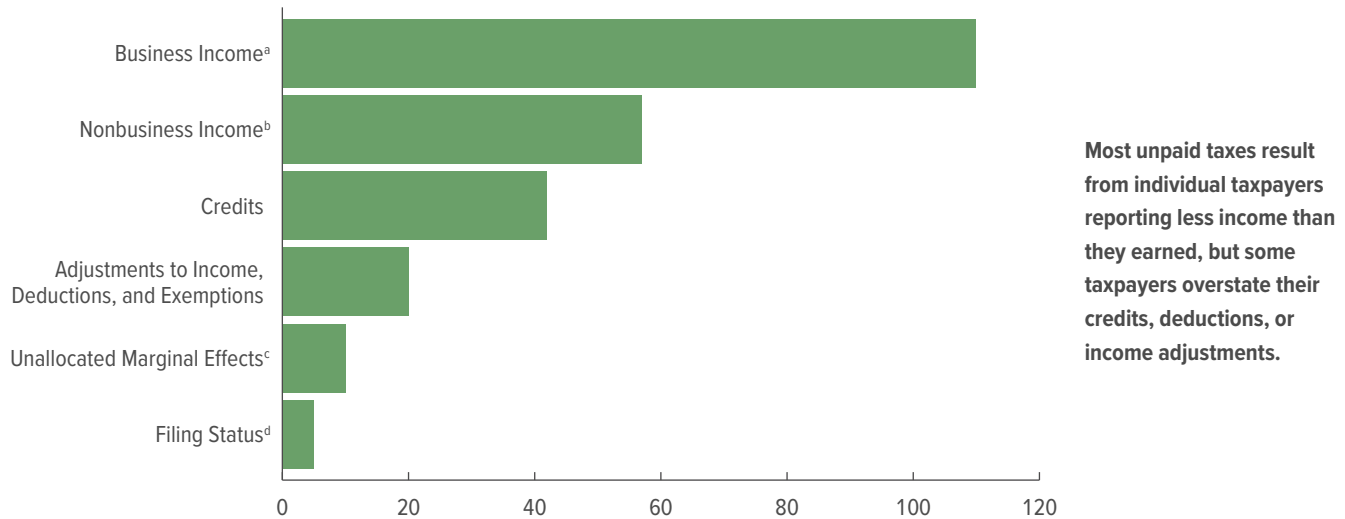
5. For example, see Joel Slemrod and others, "Does Credit-Card Information Reporting Improve Small-Business Tax Compliance?" *Journal of Public Economics*, vol. 149 (May 2017), pp. 1–19, <https://tinyurl.com/y92ew7dj>.

6. Payments reported on Form 1099-K include payments received by the taxpayer from debit, credit, or stored-value cards or from a third-party settlement organization (such as PayPal). To receive a 1099-K from a settlement organization, the taxpayer must receive gross payments in excess of \$20,000 and have more than 200 transactions. See Internal Revenue Service, "Understanding Your Form 1099-K" (March 11, 2020), <https://go.irs.gov/xwtAP>.

Figure 3.

Amount of Underreported Tax on Individual Income Tax Returns, by Type of Reporting Error

Billions of Dollars



Source: Internal Revenue Service.

The estimates are an annual average of the amount of taxes that were not paid over the 2011–2013 period.

An estimated \$1 billion in underreporting that occurs as a result of the alternative minimum tax and certain other taxes is not shown.

- a. Business income includes nonfarm proprietor income; flow-through income from partnerships, S corporations, and estates and trusts that is taxed at the individual level; rent and royalty income; and farm income. Those forms of income are reported on Schedules C, E, and F.
- b. Nonbusiness income includes wages and salaries, interest, dividends, pensions and annuities, unemployment compensation, Social Security benefits, and capital gains.
- c. Unallocated marginal effects occur when a taxpayer's underreporting of income across multiple lines of the Form 1040 would together result in a higher marginal rate than when each line is considered individually.
- d. Taxpayers may reduce the amount of tax they owe by misreporting their filing status—for example, stating that they are a “head of household” rather than “single.”

institutions are also required to report information about accounts held by U.S. citizens or entities with substantial U.S. ownership.

Income on which taxes are withheld and that third parties report to the IRS, such as wages, accounts for a very small portion of the tax gap.⁷ Withholding narrows the tax gap because it allows for the collection of tax as liability accrues. A shift in income away from wages to payments to independent contractors in the so-called gig economy could increase the tax gap because taxes

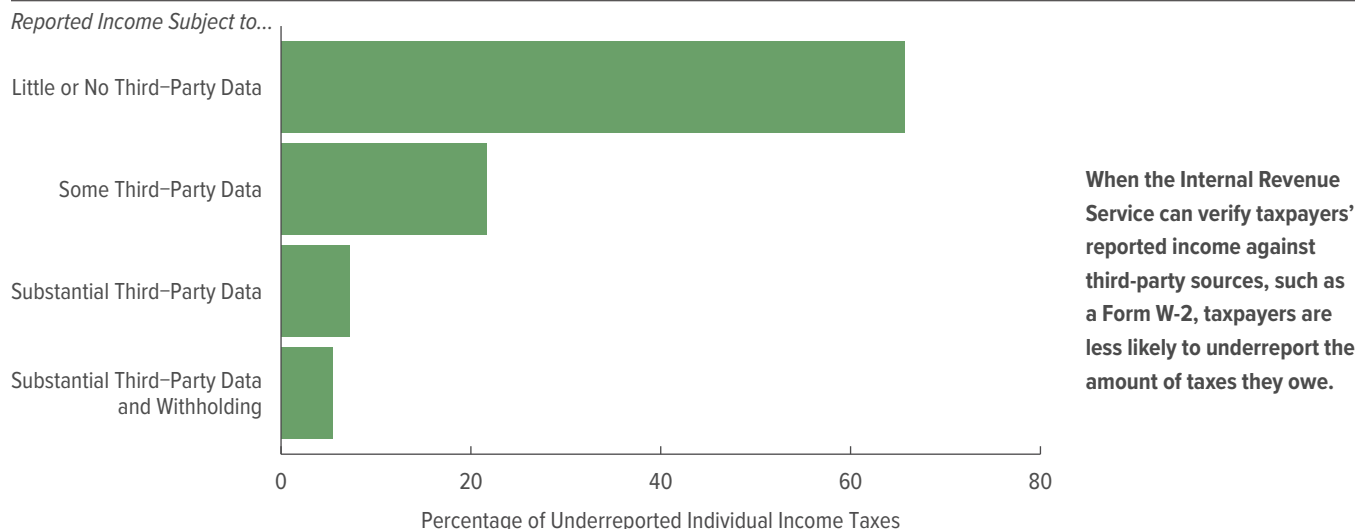
are not withheld on money paid to contractors (who are expected to remit quarterly estimated tax payments), and only certain payments are reported on Form 1099-K or on IRS Form 1099-MISC.⁸

Complexity of the Tax Code. The complexity of the tax code makes compliance more challenging and increases areas of potential dispute with the IRS. Eligibility requirements for certain tax benefits can be confusing and make it more difficult for taxpayers to determine

7. Certain types of income that are not subject to withholding may be subject to backup withholding if the payee's taxpayer identification number is incorrect or if the taxpayer has previously failed to fully report his or her income on a tax return.

8. Form 1099-MISC is generally used for reporting payments greater than \$600 to someone who is not an employee, such as someone who provides a service, or for other purposes. See Internal Revenue Service, “About Form 1099-MISC, Miscellaneous Income” (March 11, 2020), www.irs.gov/forms-pubs/about-form-1099-misc.

Figure 4.

Relationship Between Unpaid Individual Income Taxes and Third-Party Data

Source: Internal Revenue Service.

Rents, royalties, and proprietor income are subject to little or no reporting by third parties.

Capital gains, alimony income, and income from partnerships or S corporations are subject to some third-party reporting.

Pension income, unemployment compensation, dividend and interest income, and Social Security benefits are subject to substantial third-party reporting, but withholding is voluntary.

Wage and salary income is subject to substantial third-party reporting and mandatory withholding.

their tax liability.⁹ Such eligibility may also be difficult for the IRS to verify.

Another area of complexity is the varied treatment of different forms of income and expenses. For example, corporations can deduct compensation paid to employees as a business expense, but not dividends paid to employees. The difference between the corporation's interpretation and the IRS's interpretation of whether a payment is compensation or a dividend can lead to lengthy disputes that are costly for the taxpayer and the IRS.

Resources to Facilitate Compliance. Taxpayers can make mistakes filing a return or calculating liability because they do not know enough about filling out tax returns. To help taxpayers comply with tax laws, the IRS provides information through its website, in its publications, over the phone, and in local Taxpayer Assistance Centers. That assistance can narrow the gross tax gap by helping

taxpayers understand how to correctly report their income, credits, deductions, and exemptions.

Some taxpayers seek the aid of paid tax preparers to help them understand the law and how it applies to them. About half of individual income tax returns are filed by a paid preparer. The effect on compliance depends on the skill and motivation of the preparers, who have very different levels of training and expertise. Some 55 percent of all paid preparers are not regulated by the IRS or by any professional licensing board.¹⁰ Regardless of skill, the motivation of preparers may affect whether their assistance improves compliance. For example, tax preparers who offer refund-anticipation products may have

9. Complexity can also lead to taxpayers paying more than they owe. The estimated underreporting tax gap does not include such overpayments.

10. Paid preparers who are attorneys, certified public accountants, or enrolled agents must meet education requirements and pass qualifying exams to practice as tax professionals. See Internal Revenue Service, "Understanding Tax Return Preparer Credentials and Qualifications" (January 24, 2020), <https://go.usa.gov/xdsVN>; and Government Accountability Office, *Paid Tax Return Preparers: In a Limited Study, Preparers Made Significant Errors*, GAO-14-467T (April 8, 2014), Figure 2, www.gao.gov/products/GAO-14-467T.

Figure 5.

Overview of Enforcement Activities of the Internal Revenue Service

Preliminary Screening and Assessment	Examination and Document Comparison	Collection
Processing Returns <ul style="list-style-type: none"> ■ Returns screened for fraud ■ Math errors corrected 	Determining Correct Taxes <ul style="list-style-type: none"> ■ Returns selected for correspondence or field audits ■ Returns compared with third-party information for Automated Underreporter program 	Collecting Unpaid Taxes and Investigating Nonfilers <ul style="list-style-type: none"> ■ Delinquent accounts created for those who filed but did not pay full amount owed ■ Nonfiler investigations started for those who were required to file but did not

Source: Congressional Budget Office.

an incentive to claim a larger refund than the taxpayer is actually eligible for.¹¹

How the Internal Revenue Service Enforces Tax Laws

The IRS relies on a variety of approaches to reduce the tax gap. The IRS's most significant enforcement activities are examinations, collection of unpaid taxes and unfiled returns, automated screening of returns as they are filed, and comparison of information on returns with third-party information (such as that provided on Form W-2).¹² Together, those activities account for the vast majority of revenues the IRS collects after returns have been filed.¹³ Enforcement of tax laws also has an indirect effect on revenues by promoting greater voluntary compliance; however, that effect is difficult to measure.

The IRS has separate processes for determining the amount of taxes owed and for collecting unpaid taxes or unfiled returns (see Figure 5). The agency's enforcement activities are described briefly here; more detail is provided in Appendix A. IRS enforcement relies not only on

multiple approaches but also on the work of employees with various levels of skills.

Preliminary Screening and Assessment

As returns come in, the IRS screens them by using the Return Review Program, a software program that looks for indications of fraud or identity theft, and the Dependent Database, another software program that flags indications of identity theft related to the earned income tax credit (EITC) and other refundable credits. Returns that pass those filters are then screened for mathematical or clerical errors that the IRS can automatically correct.

The IRS assesses the amount of taxes due after it has processed the return and contacts the taxpayer to request additional payment or return any overpayment with a refund. If a return is then referred for examination, the assessed amount may change.

Comparison of Returns With Information From Third Parties

The IRS compares information on returns with third-party information on income that it receives from employers and payment processors. If there is a discrepancy, the IRS may contact the taxpayer to resolve it by mail through the Automated Underreporter (AUR) program, which can assess additional tax without a formal examination.

Examinations

The IRS audits some taxpayers to determine whether they accurately reported income, deductions, and credits on their return. Examiners use various criteria to determine

11. See Maggie R. Jones, *Tax Preparers, Refund Anticipation Products, and EITC Noncompliance*, CARRA Working Paper Series, Working Paper 2017-10 (Census Bureau, December 2017), <https://go.usa.gov/xdsVw> (PDF, 545 KB).

12. Other IRS enforcement activities include investigating criminal violations of internal revenue laws and other financial crimes. Estimates of the tax gap do not include taxes on income derived from illegal activities or certain types of fraud, so criminal investigations are not included in CBO's analysis of enforcement activities.

13. For a detailed chart of the tax system, see Taxpayer Advocate Service, *Publication 5341: Taxpayer Roadmap* (December 2019), www.irs.gov/pub/irs-pdf/p5341.pdf (402 KB).

which taxpayers to audit. Typically, the IRS has up to three years from a return's due date to examine it.

Collections

The IRS seeks payment of delinquent tax debts and the filing of required returns. After returns and payments have been processed, collections personnel determine whether additional taxes are due and notify taxpayers. Once an examination has concluded and taxes, penalties, and fees have been assessed, collections personnel are responsible for ensuring the amount owed is paid. The IRS also identifies taxpayers who were required to file a return but did not and follows up with those taxpayers. The IRS has the authority to place liens on a taxpayer's property or seize their property to satisfy a tax debt (including garnishing wages from employers). Typically, the IRS has up to 10 years from the date taxes are assessed to collect those taxes.

Employees' Role

Although the IRS has increased its use of automated tools, most enforcement activity relies on employees. Examinations and collection of unpaid assessments and unfiled returns require a large number of skilled employees. Three main types of employees are involved in examinations. *Tax examiners* conduct correspondence examinations for individuals and small businesses. They are trained by the agency to examine a limited range of tax topics.¹⁴ *Tax compliance officers* conduct limited-complexity, in-person examinations at IRS offices. *Revenue agents* conduct extensive, in-person field examinations at a taxpayer's home or place of business.

The two main types of collections employees are *contact representatives*, who handle taxpayer queries about automatically generated notices from the Automated Collection System, and *revenue officers*, who contact taxpayers that have not responded to notices. Contact representatives are housed in several call centers within IRS campuses; they handle cases nationwide. Revenue officers, who meet taxpayers face to face, are located throughout the country.

14. Tax examiners currently receive approximately 85 hours of training in income tax law when hired and can complete additional training modules. See National Taxpayer Advocate, Tax Law Questions, "Correspondence Examination: The IRS's Correspondence Examination Procedures Burden Taxpayers and Are Not Effective in Educating the Taxpayer and Promoting Future Voluntary Compliance," *Annual Report to Congress 2018* (February 2019), <https://taxpayeradvocate.irs.gov/2018AnnualReport>.

Indirect Effects of Enforcement

Although the IRS does not measure how much its enforcement of tax laws deters taxpayers from violating those laws, the amount of voluntary compliance probably reflects the level of enforcement activity. In a common model of compliance with tax laws, taxpayers incorporate the risk of being caught violating the laws and the severity of the punishment they might receive into their decisions.¹⁵ Taxpayers' perceptions of the risk of being caught can affect their decisions even if they themselves are not examined. (For more on how enforcement activities can deter tax noncompliance, see Box 1.)

Trends in Funding and Staffing

Nearly all of the IRS's funds are appropriated by the Congress. Appropriations for the IRS fell by about 20 percent (adjusted for inflation) between 2010 and 2019.¹⁶ About 70 percent of the IRS's overall budget is for labor. The drop in funding thus resulted in a decline in the number of IRS employees over that period, particularly in enforcement.¹⁷

Recent Appropriations

In 2019, the Congress appropriated \$11.3 billion (in current dollars) to the IRS, down from \$11.4 billion in 2018, largely allocated among four accounts:

- **Enforcement.** The largest account, at 41 percent of the IRS's appropriations in 2019, Enforcement funds the examination, collection, criminal investigation, and appeals activities. Enforcement activities rely on funds from both the Enforcement and Operations Support accounts.

15. For more discussion of how enforcement affects noncompliance, see Joel Slemrod, "Cheating Ourselves: The Economics of Tax Evasion," *Journal of Economic Perspectives*, vol. 21, no. 1 (February 2007), pp. 25–48, www.aeaweb.org/articles?id=10.1257/jep.21.1.25.

16. The analysis focuses on IRS's resources and enforcement activities from 2010 to 2018, though information going back to 2008 is also shown in figures to provide context for longer-term trends. IRS resources also declined significantly during the 1990s. For more details, see Alan Plumley and Eugene Steuerle, "Ultimate Objectives for the IRS: Balancing Revenue and Service," in Henry Aaron and Joel Slemrod, eds., *The Crisis in Tax Administration* (Brookings Institution Press, May 20, 2004), pp. 311–346, <https://tinyurl.com/ycy4m2f8>.

17. See Government Accountability Office, *Internal Revenue Service: Strategic Human Capital Management Is Needed to Address Serious Risks to IRS's Mission*, GAO-19-176 (March 2019), pp. 17–18, www.gao.gov/products/GAO-19-176.

Box 1.

Deterrent Effects of Enforcement

The enforcement activities of the Internal Revenue Service (IRS) affect revenues directly, by collecting unpaid taxes, and indirectly, by influencing taxpayers' behavior. Indirect effects are difficult to observe, and their magnitude is highly uncertain. They can be specific, influencing individuals who have been audited to change their behavior, or general, causing even taxpayers who were not audited to be more careful on their returns.

Audited taxpayers may change their behavior in positive or negative ways. They may become better informed about how to report their income and calculate their tax liability, thus increasing compliance in the future. Or they may use the opportunity to learn what the IRS is able to detect and what is permissible, which can reduce their compliance in the future. In addition, audited taxpayers may expect their audit risk to be lower in the near future, further reducing their compliance with tax laws.¹

Some researchers have found that for several years following an individual income tax audit, people tended to increase the amount of taxable wage and self-employment income they report on their tax returns.² The effects were largest for those who were assessed additional tax after the audit, and the longevity of the effect differed by income source. The researchers found a small but sustained positive effect on reported wage income over the six years following an audit. The positive effect on reported self-employment income was larger but quickly diminished. In contrast, those researchers found, corporate taxpayers tended to increase their tax aggressiveness and reduce their reported tax liability as a share of income immediately following an audit, probably because they perceived a lower audit risk in the near future.³

Taxpayers' responses may also differ based on their perceptions of an audit. Among claimants of the earned income tax

credit (EITC), audited taxpayers were less likely to claim the EITC or file taxes for a refund in subsequent years than were similar taxpayers who were not audited, even though only a small share of audited taxpayers were determined to be ineligible for the EITC.⁴ (Most audits in the analysis sample resulted in a disallowed EITC because of undeliverable mail, taxpayer nonresponse, or insufficient documentation from the taxpayer.)

Other researchers have found that higher-income taxpayers lowered their reported income and tax liability after being notified that they would face an audit, perhaps because they viewed the eventual audit as a negotiation. (Lower-income taxpayers tended to increase their reported income after being notified of an audit.)⁵

Taxpayers may be more likely to comply with tax laws if they perceive a higher risk of being caught, even if they are not audited themselves. Among corporate taxpayers, an increase in the overall examination rate increased all taxpayers' reported effective tax rate.⁶ Researchers have analyzed data from an experiment in which randomly selected firms with a high risk of noncompliance were contacted by the IRS. They found that although IRS contact increased the amount of employment tax remittances paid by other businesses with the same tax preparer, it also decreased remittances by subsidiaries of the contacted firm. In that analysis, on net, the indirect effects of such contact on the people who shared a tax preparer, ownership link, or geographic area with the contacted taxpayer were close to zero.⁷

1. For an overview of recent studies on tax compliance, see Joel Slemrod, *Tax Compliance and Enforcement*, Working Paper 24799 (National Bureau of Economic Research, July 2018), p. 924, www.nber.org/papers/w24799.

2. See Jason DeBacker and others, "Once Bitten, Twice Shy? The Lasting Impact of Enforcement on Tax Compliance," *The Journal of Law and Economics*, vol. 61, no. 1 (February 2018), pp. 1–35, <https://doi.org/10.1086/697683>.

3. See Jason DeBacker and others, "Legal Enforcement and Corporate Behavior: An Analysis of Tax Aggressiveness After an Audit," *The Journal of Law and Economics*, vol. 58, no. 2 (May 2015), pp. 291–324, <http://dx.doi.org/10.1086/684037>.

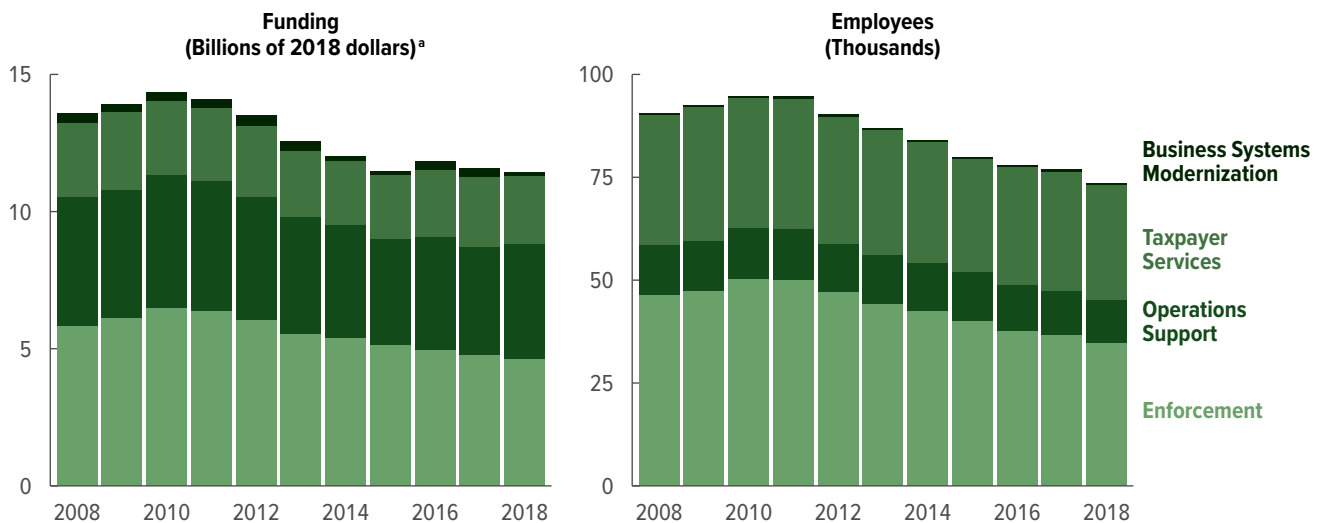
4. See John Guyton and others, *The Effects of EITC Correspondence Audits on Low-Income Earners*, Working Paper 24465 (National Bureau of Economic Research, May 2019), www.nber.org/papers/w24465.

5. Joel Slemrod, Marsha Blumenthal, and Charles Christian, "Taxpayer Response to an Increased Probability of Audit: Evidence From a Controlled Experiment in Minnesota," *Journal of Public Economics*, vol. 79, no. 3 (March 2001), pp. 445–483, [https://doi.org/10.1016/S0047-2727\(99\)00107-3](https://doi.org/10.1016/S0047-2727(99)00107-3).

6. See Jeffrey L. Hoopes, Devan Mescall, and Jeffrey A. Pittman, "Do IRS Audits Deter Corporate Tax Avoidance?" *The Accounting Review*, vol. 87, no. 5 (2012), pp. 1603–1639, <https://doi.org/10.2308/accr-50187>; and Jason DeBacker and others, "Legal Enforcement and Corporate Behavior: An Analysis of Tax Aggressiveness After an Audit," *The Journal of Law and Economics*, vol. 58, no. 2 (May 2015), pp. 291–324, <http://dx.doi.org/10.1086/684037>.

7. See William C. Boning and others, *Heard it Through the Grapevine: Direct and Network Effects of a Tax Enforcement Field Experiment*, Working Paper 24305 (National Bureau of Economic Research, February 2018), www.nber.org/papers/w24305.

Figure 6.

Funding and Number of Employees of the Internal Revenue Service, by Appropriation Account

Source: Congressional Budget Office, using data from the Internal Revenue Service.

Employees are measured as the number of full-time equivalents (FTEs). Because not all employees work full time in a given year, the Internal Revenue Service calculates the number of FTEs as the total number of hours worked divided by the number of hours that a full-time employee would work.

a. Appropriations are expressed in 2018 dollars using a combination of the employment cost index for wages and salaries and the chain-weighted gross domestic product price index, based on the share of labor and nonlabor costs.

- **Operations Support.** Agencywide expenses for office space, information technology maintenance and security, research, and strategic planning are funded by the Operations Support account, which received 35 percent of the IRS's appropriations in 2019.
- **Taxpayer Services.** The Taxpayer Services account funds the infrastructure necessary for processing returns and refunds, as well as assistance and education for taxpayers as they prepare to file. It was allocated 23 percent of the IRS's appropriations in 2019.
- **Business Systems Modernization.** This account funds upgrades to the agency's taxpayer account and e-filing technology systems. Appropriations to this account in 2019 were 1 percent of the agency's total appropriations.

Appropriations in 2020 are roughly the same as those in 2019.

Appropriations From 2010 to 2018

Appropriations to the IRS over the past 10 years peaked in 2010, measured in both nominal (current) and real

2018 dollars (see Figure 6).¹⁸ Between 2010 and 2018, the agency's appropriations decreased by 20 percent, measured in real dollars.¹⁹ The Enforcement account absorbed much of that decline in funding—a 29 percent drop in real resources during that period.

Moving appropriated funds between the IRS's four accounts requires Congressional approval, though the agency has the flexibility to direct user fees and reimbursements for providing services to other agencies to any account. User fees and reimbursements added less than \$0.5 billion to the IRS's budget in 2018.

18. In CBO's baseline projections, the agency adjusts discretionary funding related to federal personnel with the employment cost index for wages and salaries, and it adjusts other discretionary funding with the GDP price index. IRS appropriations in this report are adjusted for inflation with a blend of those indexes, weighted to reflect the percentage of each appropriation account that funds personnel.

19. The analysis here is based on the *Internal Revenue Service Data Book*, so the period ends with the last published year of data at the time of writing (2018). During this period, the IRS's responsibilities have grown. For more discussion, see Brian Erard and Alan Plumley, "Doing More With Less? Using Data and Analytics to Overcome Shrinking Enforcement Budgets and Expanding Responsibilities" (paper presented at the 2018 Corporate Tax Management Conference on Tax and Technology), <https://tinyurl.com/y78ocq3c>.

Staffing

Because labor costs account for much of the IRS's budget, the IRS reduced its staff by instituting a hiring freeze in 2011 and offering buyouts for early retirement in 2012. The result was a decline of 22 percent in the number of employees from its 2010 peak to 2018, mostly from attrition.

Employees funded by the Enforcement account absorbed much of the decline in IRS personnel: a 31 percent reduction in employees between 2010 and 2018.²⁰ Employees who work the most complex examination and collections cases experienced especially large declines. Between 2010 and 2018, the number of revenue agents, who handle complex enforcement cases, fell by 35 percent, and the number of revenue officers, who manage difficult collections cases, dropped by 48 percent (see Figure 7).

Trends in Enforcement

The loss of 15,000 enforcement employees between 2010 and 2018 led to a significant reduction in the number of examinations and the number of follow-ups on discrepancies between returns and third-party data, as well as an increase in assessments that were not collected and unfiled returns that were not secured. Over that period, the number of examinations dropped by about 40 percent even as the number of returns filed grew by 5 percent.

Income tax returns filed by individuals and corporations account for the bulk of recommended additional tax from examination. The decline in examination rates for income tax returns over the 2010–2018 period led to a drop in the total amount of additional tax the IRS recommended following examinations. Taxpayers' appeals of recommended additional taxes, which can affect the amount of revenues from examinations, remained a constant share of examinations.

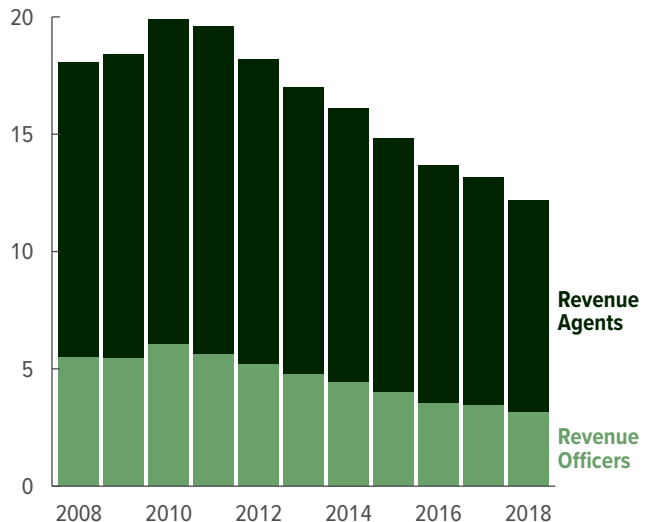
Examinations of Individual Income Tax Returns

The examination rate for individual income tax returns declined from 1.1 percent to 0.6 percent from 2010 to

Figure 7.

Employees in Selected Enforcement Positions

Thousands of Employees



The number of experienced, highly skilled employees working in examinations (revenue agents) and collections (revenue officers) declined by 35 percent and 48 percent, respectively, from 2010 to 2018.

Source: Congressional Budget Office, using data from the Internal Revenue Service.

Employees are measured as the number of full-time equivalents (FTEs). Because not all employees work full time in a given year, the Internal Revenue Service calculates the number of FTEs as the total number of hours worked divided by the number of hours that a full-time employee would work.

2018 (see Figure 8).²¹ Most examinations of individual returns are conducted through correspondence, and the share of examinations handled through correspondence did not change significantly as the total number of examinations declined.

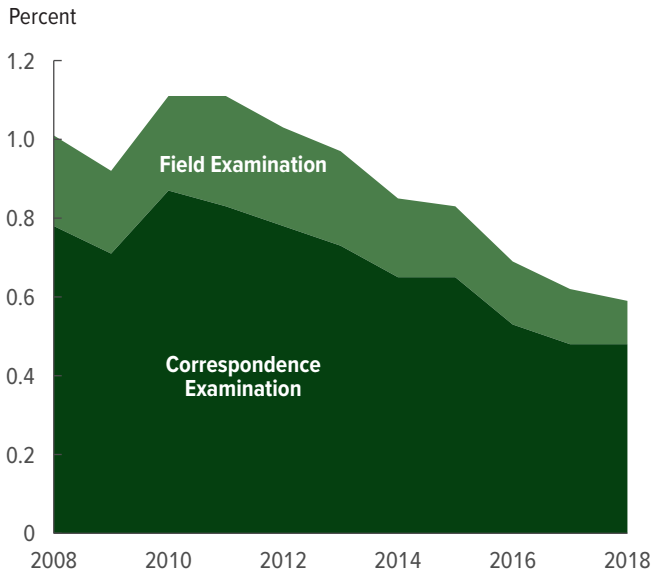
The percentage decline in the examination rate was larger for higher-income returns. For returns with more than \$1 million in total income (before losses were deducted), the examination rate dropped from 8 percent in 2010 to 3 percent in 2018, a 63 percent decline (see Figure 9). The examination rate for returns with total positive income of less than \$200,000, accounting for over

20. The *Internal Revenue Service Data Book* lists employees at the level of "budget activity," a subcategory of appropriation account. The Enforcement account funds three budget activities: examinations and collections, investigations, and regulatory. See Internal Revenue Service, *Internal Revenue Service Data Book, 2018* (June 30, 2020), <https://go.usa.gov/xfcy3>.

21. The examination rate is calculated as the number of examinations closed in a fiscal year divided by the number of returns filed in the previous calendar year. That is because most examination activity takes place in the fiscal year after a return is filed.

Figure 8.

Examination Rate for Individual Returns, by Type of Examination



Source: Congressional Budget Office, using data from the Internal Revenue Service.

The examination rate is the number of examinations of individual returns that were closed in a particular fiscal year divided by the number of individual returns filed in the previous calendar year.

Field examinations are extensive in-person audits conducted at a taxpayer's home or place of business. Correspondence examinations of individuals or small businesses do not involve visits to the taxpayer and are generally conducted by mail.

95 percent of individual returns each year, dropped to 0.6 percent in 2018 from 1.0 percent in 2010, a 45 percent decline.

Over one-third of all individual returns selected for examination in 2018 were chosen because they included an EITC claim.²² A former IRS commissioner noted that tax law related to the EITC is so complex that “even people trying to complete the returns accurately and their

preparers have trouble figuring out who gets credit.”²³ That complexity, combined with the focus during the past decade on reducing improper payments by government programs, has kept examination rates high for returns with EITC claims.²⁴ (See Box 2 for more information.) The examination rate for returns with EITC claims is higher than for other returns that report less than \$200,000 in total income, though the difference between the examination rates for those groups declined to 1.0 percentage point in 2018, from 1.7 percentage points in 2010 (see Figure 10 on page 15).

Examinations of Corporate Income Tax Returns

The examination rate for corporate income tax returns dropped to 0.9 percent in 2018 from 1.4 percent in 2010 (see Figure 11 on page 16). Because of their complexity, most corporate income tax examinations are conducted in the field. Although the total number of corporate income tax examinations has declined, the share of examinations conducted in the field—that is, at the taxpayer's home or workplace—has been roughly constant.

The rate of examination for corporations that reported assets of \$20 billion or more declined to about 50 percent in 2018, down from almost 100 percent in 2010 (see Figure 12 on page 17). For corporations with assets of less than \$10 million, the examination rate fell to 0.6 percent from 1.1 percent.²⁵

23. See William Hoffman, “A Conversation With Former IRS Commissioner John Koskinen: Tax Administration,” Part 1, *Tax Notes Talks* (podcast, October 10, 2019), <https://tinyurl.com/s6t8phd>.

24. For the EITC, the amount of credit that is either claimed by an ineligible taxpayer or claimed in the wrong amount by an eligible taxpayer is considered an improper payment. The amount of EITC that is not claimed by eligible taxpayers is not included in that calculation.

25. The examination rate is calculated as the number of examinations closed in a fiscal year divided by the number of returns received in the previous calendar year. As a result, the rate can exceed 100 percent in a given year, if older returns are examined in the current fiscal year or if an examination started in a prior year takes longer than a year to close, as complex corporate examinations typically do. In some situations, the IRS examines multiple years of a corporation's returns and then closes all of them at one time. In 2012, the examination rate for corporations with assets reported on their balance sheets of \$20 billion or more surpassed 100 percent.

22. The percentage of returns in a fiscal year that were examined because of an EITC claim is drawn from the *Internal Revenue Service Data Book* and divided by the number of returns filed the previous calendar year. See Internal Revenue Service, *Internal Revenue Service Data Book, 2018* (June 30, 2020), <https://go.usa.gov/xfcy3>.

Additional Taxes Recommended Following Examinations

Examinations generate enforcement revenue by proposing adjustments to a return and recommending additional tax and penalties, though a small number of cases result in a refund for the taxpayer. After a period when a taxpayer may challenge or appeal the audit findings, that additional tax is no longer recommended but required and becomes a tax assessment. As examinations declined, the total amount of additional tax (excluding penalties) recommended for individual and corporate income tax returns fell by 50 percent, from \$46 billion in 2010 to \$23 billion in 2018.

The amount of additional tax recommended after examinations of individual income tax returns fell steadily over the 2010–2018 period (see Figure 13 on page 18). The average amount of additional tax that the IRS recommended did not change significantly, but the number of examinations declined. The decline was largest for taxpayers with income of \$1 million or more (before losses, exclusions from income, or adjustments to income). The amount of additional tax recommended for that group fell to \$1.9 billion in 2018 from \$5.7 billion in 2010.

For corporations, the amount of additional tax recommended after examinations declined more steeply and was more volatile. That result was driven by examinations of corporations with more than \$20 billion in assets because the closure of a few big cases can account for a large percentage of the total amount of additional tax recommended. In 2017, the closure of a small number of large corporate cases accounted for more than \$2 billion in examination assessments.²⁶

Appeals of Recommended Additional Taxes and Penalties

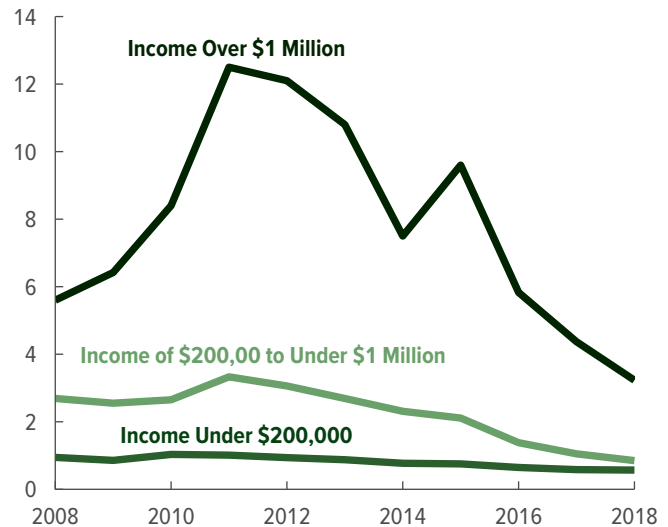
Taxpayers have the right to challenge a recommendation of additional tax and penalties, either through an administrative appeal within the IRS or through a judicial appeal in the U.S. Tax Court, a U.S. District Court, or the U.S. Court of Federal Claims. A verdict can reduce or eliminate the additional tax. If the additional tax is reduced, any penalties that were calculated based on the amount of that tax are reduced as well. Courts may also

26. See Treasury Inspector General for Tax Administration, *Trends in Compliance Activities Through Fiscal Year 2017*, Reference Number 2017-30-072 (September 13, 2018), p. 6, <https://go.usa.gov/xdHjC> (PDF, 1 MB).

Figure 9.

Examination Rate for Individual Returns, by Amount of Income

Percentage of Returns



Source: Congressional Budget Office, using data from the Internal Revenue Service.

Income is total positive income (TPI), which is the sum of wages and salaries, interest, dividends, income from profitable businesses, and income from investment. TPI differs from adjusted gross income in that exclusions and deductions are not subtracted and most losses from business and investment are excluded.

The examination rate is the number of examinations of individual returns that were closed in a particular fiscal year divided by the number of individual returns filed in the previous calendar year.

reduce penalties independently, without changing the amount of additional tax, if taxpayers can show reasonable cause for not complying with tax law.

The overall number of appeals declined from 2010 to 2018, but the rate at which individual and corporate taxpayers challenged the results of their examinations did not change significantly over the period.²⁷ Many factors may influence a taxpayer's decision to challenge an examination result: the strength of the IRS's case, the scope of the changes the IRS made to the return, the amount of additional tax the IRS recommended, and the taxpayer's resources (for example, funds may be needed to hire assistance in the administrative or judicial appeals process). Any changes in these factors over the period did

27. See Internal Revenue Service, *Internal Revenue Service Data Book, 2010–2018* (June 30, 2020), <https://go.usa.gov/xfcy3>.

Box 2.

Improper Payments and the Earned Income Tax Credit

The earned income tax credit (EITC) for low-income taxpayers is a refundable tax credit—that is, if the amount of the credit exceeds a filer's tax liability, the taxpayer receives the excess amount. In 2018, claims for the EITC amounted to \$73.6 billion.¹ The government paid nearly 80 percent of that total, \$58.6 billion, to individuals whose returns showed that their tax liability was less than the amount of the credit.²

Some of those EITC payments were improper because they were made to taxpayers who were ineligible for the credit or because the government paid the wrong amount to eligible recipients. Improper payments, which cost the government an estimated \$140 billion in 2017, have been a focus of legislation and executive action for over a decade.³ The Improper Payments Information Act of 2002, as amended by the Improper Payments Elimination and Recovery Act of 2010 and the Improper Payments Elimination and Recovery Improvement Act of 2012, increased federal agencies' requirements to report improper payments. The act also required the director of the Office of Management and Budget to work with agencies to target the small subset of programs, including the EITC, that account for the majority of improper payments. Those high-priority programs must report additional information on the improper payments they issued and establish annual goals for reducing such payments.⁴

To comply with reporting requirements, the Internal Revenue Service (IRS) uses the results of random audits from the National Research Program (NRP) to estimate the percentage of improper EITC claims. In 2018, the IRS estimated that 25 percent (\$18.4 billion) of the \$73.6 billion in EITC claims was improper. It recovered \$1.2 billion of those improper payments through post-refund enforcement activity.⁵ The NRP sample revealed no instance of an underpayment to taxpayers who claimed the credit. However, many eligible taxpayers fail to claim the EITC, and nonpayments to such taxpayers are not incorporated in calculations of improper payments.

The high rate of improper EITC claims has several causes. The credit's eligibility requirements are complex, and the IRS lacks third-party data to authenticate much of what taxpayers report to support their claim (for example, a child's residence throughout the year or a taxpayer's marital status.) That lack of data limits the IRS's ability to verify eligibility without conducting an audit, and some taxpayers may not be able to provide documentation to prove their eligibility. The population that is eligible to claim the EITC undergoes significant turnover each year because wages and family circumstances change, so sending potential claimants notices to encourage compliance is difficult.⁶ Finally, taxpayers who claim the EITC are more likely than other filers to use paid return preparers who are not subject to the education requirements or qualifying examinations of tax professionals.⁷

1. See Department of the Treasury, *Agency Financial Report: Fiscal Year 2018*, p. 194, <https://go.usa.gov/xdHWa> (PDF, 9.8 MB).

2. See Department of the Treasury, "Payment where Earned Income Credit Exceeds Liability for Tax," *Budget for Fiscal Year 2020 Appendix*, p. 953, <https://go.usa.gov/xdHWb> (PDF, 572 KB).

3. See Garrett Hatch, *Improper Payments in High-Priority Programs: In Brief*, Report for Congress R45257, Congressional Research Service (July 2018), <https://go.usa.gov/xwtFa>.

4. Consistent with previous estimates, the Treasury uses EITC claims—including those that reduce the amount of tax paid—to estimate improper payments (though only the government's outlays meet the definition of an improper payment).

5. If the \$1.2 billion in recovered improper EITC payments was subtracted before calculating the improper payment rate, that rate would be 23.4 percent rather than the reported 25.1 percent. (Those estimates are based on NRP data; revenue recovered from operational audits involving the EITC is excluded.) See Department of the Treasury, *Agency Financial Report: Fiscal Year 2018*, footnote 4, p. 194, <https://go.usa.gov/xdHWa> (PDF, 9.8 MB).

6. See Department of the Treasury, "Barriers," *Agency Financial Report: Fiscal Year 2018*, Section III, p. 200, <https://go.usa.gov/xdHWa> (PDF, 9.8 MB).

7. See Internal Revenue Service, *Compliance Estimates for the Earned Income Tax Credit Claimed on 2006–2008 Returns*, Publication 5162 (August 2014), Table 8, <https://go.usa.gov/xdFnn> (PDF, 972 KB).

not significantly affect the rate at which taxpayers agreed to examination results.²⁸

28. A study examining the outcomes of appeals by large public corporations found that as the IRS's resources for conducting corporate examinations declined, the IRS may have prioritized examinations of large corporate taxpayers with weaker (more

questionable) cases. Despite such prioritization, the study found that the reduction in the IRS's resources had a negative impact on the amount of tax revenue it received from large corporations. See Michelle Nessa and others, "How Do IRS Resources Affect the Corporate Audit Process?" *The Accounting Review*, vol. 95, no. 2 (March 2020), pp. 311–338, <https://dx.doi.org/10.2308/acct-52520>.

Automated Enforcement Activity

The IRS does not rely entirely on formal examinations to make adjustments to tax liability. Some processes to check the accuracy of returns are largely automated and thus require fewer employee hours per return than an examination. They include the correction of mathematical and clerical errors and the identification of discrepancies between returns and third-party documents.

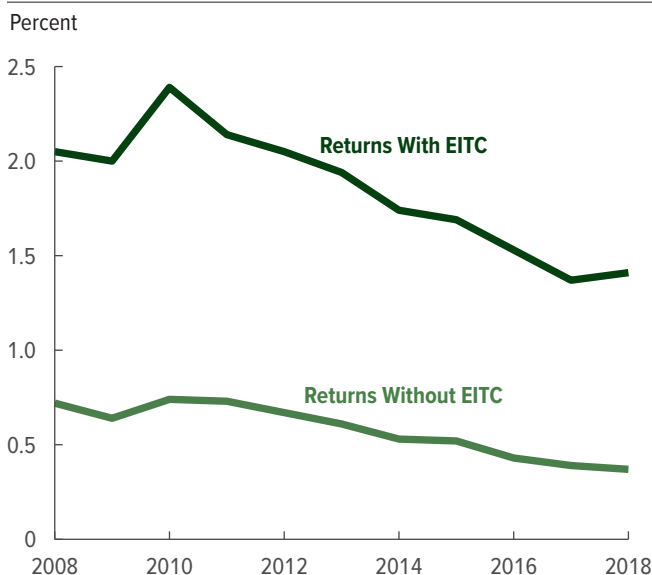
The IRS is authorized by law to automatically correct certain mathematical and clerical errors on returns and recalculate liability on the basis of such corrections. That “math error authority” is applied using computer software. The number of errors corrected automatically by the agency each year depends on the number and type of errors the IRS is authorized by the Congress to correct and the number of taxpayers who made them. In 2018, 1.9 percent of individual returns were corrected automatically with math error authority. The IRS’s math error authority was expanded in 2009 to enable it to automatically correct certain errors associated with the temporary Making Work Pay and Recovery Rebate credits.²⁹ If errors associated with those credits are set aside, the number of math errors identified as a share of individual income tax returns declined from 2010 to 2018. That decline occurred because taxpayers made fewer correctable errors rather than because the IRS’s resources were constrained.

The IRS uses software after it processes returns to identify discrepancies between those returns and data supplied by employers and other third parties. Some discrepancies are selected for review as part of the Automated Underreporter program, which generates notices to taxpayers when a discrepancy is found in a return, proposing changes to the return based on the third-party information. The number of such notices depends on the number of AUR personnel available to review the flagged returns and handle taxpayers’ responses to notices. The number of employees in the AUR program declined by 40 percent, from 2,255 to 1,366, between 2010 and 2018. Improvements in the selection of cases to be reviewed allowed the IRS to increase the productivity of the AUR program’s remaining employees, but

29. Errors associated with the Making Work Pay and Recovery Rebate credits (authorized in the American Recovery and Reinvestment Act of 2009) totaled 10 million on returns filed in calendar year 2009 (7 percent of returns) and 7 million on returns filed in calendar year 2010 (5 percent of returns). Such errors continued to decline in later years.

Figure 10.

Examination Rate for Certain Returns With and Without the Earned Income Tax Credit



Source: Congressional Budget Office, using data from the Internal Revenue Service.

The examination rate is the number of examinations of individual returns that were closed in a fiscal year divided by the number of individual returns filed in the previous calendar year.

Income is total positive income (TPI), which is the sum of wages and salaries, interest, dividends, income from profitable businesses, and income from investment. TPI differs from adjusted gross income in that exclusions and deductions are not subtracted and most losses from business and investment are excluded. The figure shows the rate of examination for all taxpayers with TPI of less than \$200,000.

EITC = earned income tax credit.

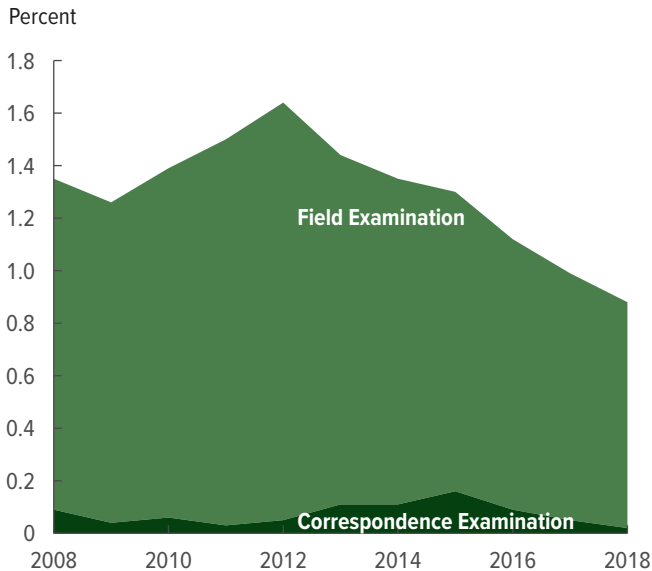
case closures nonetheless declined as a share of individual returns by 36 percent over the period (see Figure 14 on page 19).³⁰

Collections Revenues

In 2018, taxpayers owed the IRS about \$511 billion in delinquent tax debt, or unpaid assessments (see Figure 15 on page 20, top panel). Unpaid assessments arise when taxpayers file a return without paying taxes owed in full, when examinations or automated enforcement activity result in additional tax that is not paid promptly,

30. See Treasury Inspector General for Tax Administration, “Automated Underreporter Program Tax Assessments Have Increased Significantly; However, Accuracy-Related Penalties Were Not Always Assessed When Warranted,” Reference Number 2015-30-037 (May 8, 2015), pp. 5–6, <https://go.usa.gov/xdHTTr>.

Figure 11.

Examination Rate for Corporate Returns, by Type of Examination

Source: Congressional Budget Office, using data from the Internal Revenue Service.

The examination rate is the number of examinations of corporate returns that were closed in a particular fiscal year divided by the number of corporate returns filed in the previous calendar year.

Field examinations are extensive in-person audits conducted at a taxpayer's home or place of business. Correspondence examinations of individuals or small businesses do not involve visits to the taxpayer and are generally conducted by mail.

Forms 1120-S (filed by S corporations) are excluded from the calculation of corporate returns.

or when nonfilers are found to owe taxes. They include taxes and accrued penalties and interest for the current year, as well as any amounts owed from previous years that fall within the 10-year statute of limitations on collecting taxes.³¹ Only a portion of unpaid assessments is collectible; in some cases, the taxpayer cannot be located, is deceased (or, in the case of a business, defunct), or faces financial hardship.

31. Amounts assessed following examination that the taxpayer does not agree with and amounts in appeals are also included. Treasury estimates that about 14 percent of the unpaid assessments in fiscal year 2016 were from examinations. For more details on unpaid assessments, see Treasury Inspector General for Tax Administration, *Trends in Compliance Activities Through Fiscal Year 2016*, Reference Number 2017-30-072 (September 11, 2017), <https://go.usa.gov/xdHjh> (PDF, 3.95 MB).

The economy thus affects collections revenues—the tax, penalties, and interest that are received as a result of collections activity on returns filed with additional tax due or on overdue returns.³² A stronger economy not only increases tax liabilities but can also result in fewer uncollectible assessments. The combination of those factors suggests that in a growing economy, the IRS would collect a greater share of unpaid assessments. However, although the economy grew stronger between 2010 and 2018, revenues from enforcement activities increased only slightly. Between 2010 and 2018, collections revenue was within 8 percent to 10 percent of the growing amount of unpaid assessments owed to the IRS. (See Figure 15 on page 20, center and bottom panels).

Collections Activity

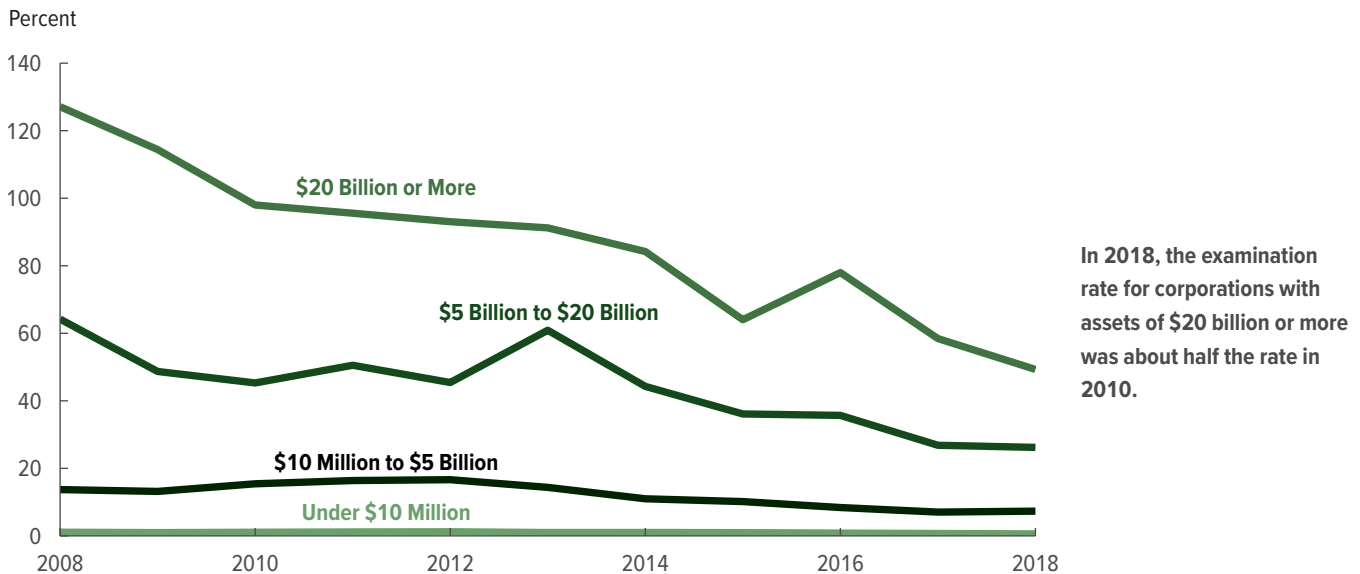
Most cases in collection are delinquent accounts from filers who either did not pay the tax they owed or paid only a portion of the amount due (see Figure 16 on page 21). From 2010 to 2018, the IRS typically opened more delinquent account cases in a year than it closed, leading to a growing backlog. In recent years, the agency has transferred some accounts in the backlog to private collection agencies, leading to the closure of more cases.

Another set of cases in collection are investigations of people who did not file a return. The IRS identifies probable nonfilers through third-party information or prior-year filing information and sends them an automated notice about their failure to file. The number of notices sent has declined in recent years because the reduction in the IRS's resources meant that fewer employees were available to identify nonfilers.

The decline in staff has also meant that there is little follow-up on the notices sent to nonfilers. The IRS assesses tax on nonfilers with an automated process that creates a substitute return with data from third parties

32. Some tax debt is paid by transferring credits (for example, a refund on income taxes paid) to satisfy a debt from a past year. Collections revenue is the amount of delinquent tax debt collected excluding such transfers plus the amount of payments from investigations of nonfilers. See Internal Revenue Service, *Internal Revenue Service Data Book, 2018* (June 30, 2020), <https://go.usa.gov/xfcy3>. The figure for delinquent tax debt is drawn from the amount of gross accounts receivable calculated by the IRS Office of Research, Analysis, and Statistics and Chief Financial Officer. See Treasury Inspector General for Tax Administration, *Trends in Compliance Activities Through Fiscal Year 2018*, Reference Number 2019-30-063 (September 9, 2019), Appendix IV, Figure 2, <https://go.usa.gov/xwMEW> (PDF, 729 KB).

Figure 12.

Examination Rate for Corporate Returns, by Amount of Assets

Source: Congressional Budget Office, using data from the Internal Revenue Service.

The examination rate is the number of examinations of corporate returns that were closed in a particular fiscal year divided by the number of corporate returns filed in the previous calendar year. The rate can exceed 100 percent if returns received prior to the previous calendar year are selected for audit or if an audit has not closed by the subsequent fiscal year.

Forms 1120-S (filed by S corporations), 1120-C (filed by cooperative associations), and 1120-F (filed by foreign corporations with U.S. income) are excluded from the calculation of corporate returns.

Also excluded are returns filed by corporations with total receipts and total assets of less than \$250,000 at the end of the tax year. Those corporations are not required to provide a summary of their balance sheet (which lists assets and liabilities at a point in time) with their return.

(the Automated Substitute for Return, or ASFR). Even though substitute returns are created automatically, employees are necessary to respond to taxpayers who offer reasons for not filing or who want to correct the substitute returns, which tend to overstate taxpayers' liability. The number of ASFR cases closed declined to 10,000 in 2018 from 1.2 million in 2010, and the program has been largely inactive since 2015, when the IRS assigned most of the ASFR's staff to other functions.³³ With the reduction in ASFR activity, enforcement activity for many high-income nonfilers has been reduced to a series of notices.³⁴

33. See Treasury Inspector General for Tax Administration, *A Significantly Reduced Automated Substitute for Return Program Negatively Affected Collection and Filing Compliance*, Reference Number 2017-30-078 (September 29, 2017), pp. 9–10, <https://go.usa.gov/xdHTt> (PDF, 990 KB).

34. See Treasury Inspector General for Tax Administration, *High-Income Nonfilers Owing Billions of Dollars Are Not Being Worked by the Internal Revenue Service*, Reference Number 2020-30-015 (May 29, 2020), <https://go.usa.gov/xwGuy> (PDF, 3.9 MB).

Impact of the Coronavirus Pandemic on Enforcement

The disruptions stemming from the 2020 coronavirus pandemic will reduce the ability of the IRS to enforce tax laws and will present new challenges for taxpayers in complying with tax laws.

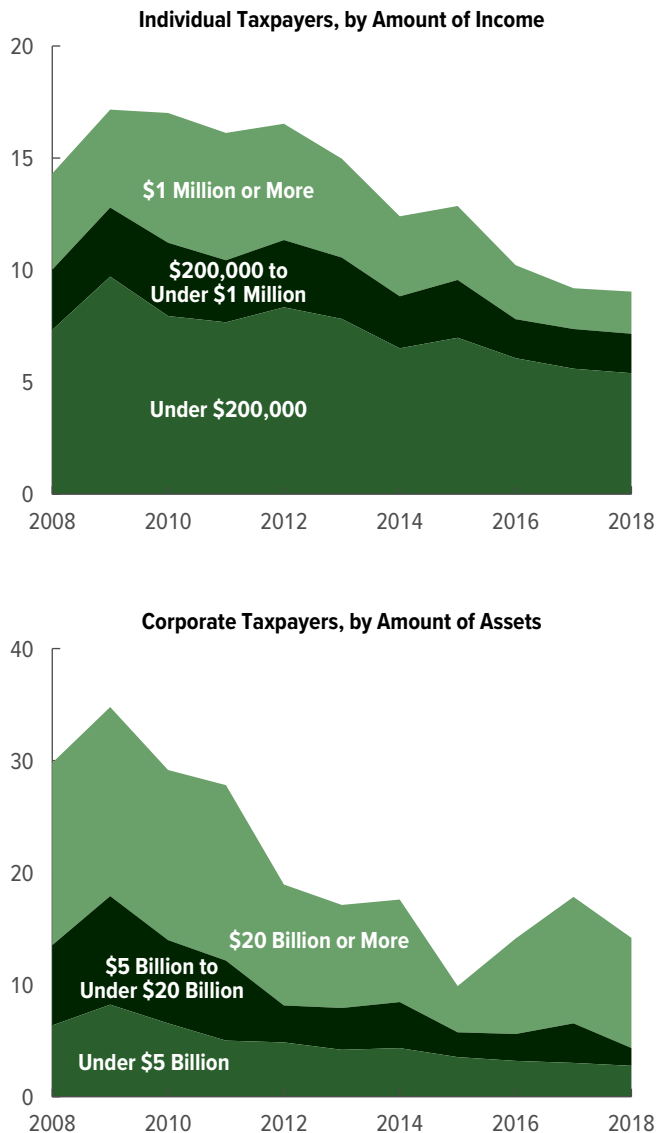
Reduced Enforcement Activities. The IRS announced a pause in many enforcement activities from April 1, 2020, through July 15, 2020.³⁵ Specifically, the IRS suspended liens and levies, stopped initiating new field or correspondence examinations, and extended deadlines to make payments on installment agreements and submit supporting documentation for EITC claims. In addition, the closure of IRS facilities has interrupted the processing of paper correspondence from taxpayers, including documents related to audit and collections activities.

35. See Internal Revenue Service, "IRS Unveils New People First Initiative; COVID-19 Effort Temporarily Adjusts, Suspends Key Compliance Program," IR-2020-59 (news release, March 25, 2020), <https://go.usa.gov/xvQf4>.

Figure 13.

Amount of Additional Tax Recommended After Audits

Billions of Dollars



As the examination rate dropped, the amount of additional tax recommended after audits also declined.

Source: Congressional Budget Office, using data from the Internal Revenue Service.

Increased Demands for Taxpayer Services and Operations. The IRS extended the April 15 deadline to file and pay federal income taxes to July 15, 2020, so the IRS will need to devote additional resources to processing tax returns and refunds over a longer time

period. In addition, the agency has been tasked with administering the individual recovery rebates enacted as part of the Coronavirus Aid, Relief, and Economic Security (CARES) Act.³⁶ The IRS has disbursed those payments quickly—in the two months after enactment of the CARES Act, the IRS paid nearly \$267 billion to 159 million individuals.³⁷ Those rebates and other new tax provisions will create further demands on IRS resources when 2020 tax returns are filed in 2021.

Reduced Taxpayer Assistance. The IRS suspended live telephone assistance and closed the walk-in Taxpayer Assistance Centers, reducing the resources available to help taxpayers comply with the law. Those actions will hinder taxpayers seeking assistance with new issues that have arisen from recent legislative and administrative changes as well as taxpayers whose issues predate the coronavirus pandemic.

How Changes in Funding Would Affect Future Revenues

Policymakers have expressed interest in how increases in IRS funding, particularly for enforcement activities, would increase tax revenues. (For a discussion of other changes that could increase revenues under the current tax regime, see Box 3 on page 22.) Estimates of the additional revenue that would result from more spending—such as the estimates in this report—would not be included in a cost estimate because of scorekeeping guidelines used by the Congress.³⁸ If additional funds were appropriated, however, their effects on both spending and revenues would be incorporated into the Congressional Budget Office's next budget baseline. The estimates are necessarily uncertain because the link between spending on enforcement and the collection of revenues is not direct, and many factors can affect the IRS's ability to use added funding to increase revenues.

36. The IRS received an additional \$250 million in appropriations for fiscal year 2020 in the CARES Act (Public Law 116-136) to facilitate the extension of the filing season and processing of the recovery rebates.

37. See Internal Revenue Service, "159 Million Economic Impact Payments Processed; Low-Income People and Others Who Aren't Required to File Tax Returns Can Quickly Register for Payment With IRS Non-Filers Tool," IR-2020-111 (news release, June 3, 2020), <https://go.usa.gov/xwBWP>.

38. CBO previously estimated the revenue effects of increased appropriations for IRS enforcement. See Congressional Budget Office, *Options for Reducing the Deficit: 2019–2028* (December 2018), p. 306, www.cbo.gov/publication/54667.

Estimated Effect on Revenues of Two Options to Increase Funding

CBO estimated the effect of increasing the IRS's enforcement budget by \$20 billion or \$40 billion over a 10-year period, projecting how much of the additional revenue would be received in each year. Those estimates are based on the IRS's estimates of the average amount of revenue that would be collected for every additional dollar of enforcement. However, CBO has not estimated the deterrent effect of increased enforcement on other taxpayers—and thus its estimates do not show increases in revenues as greater enforcement influences more taxpayers to comply with tax laws.

Estimated Revenue Effects of a \$20 Billion Increase.

CBO estimates that a \$20 billion increase to the IRS's appropriations for enforcement activities over 10 years would raise revenues by \$61 billion over that period. On net, the increase in spending on enforcement would reduce the deficit by \$41 billion over the 2021–2030 period (see Table 1 on page 23).³⁹

The IRS's funding would increase gradually, rising by \$500 million each year for the first five years, and then remain at an additional \$2.5 billion per year from 2026 to 2030.⁴⁰ Each infusion of new funding would result in the start of new enforcement initiatives—expansions of audits and other activities that could improve compliance with the tax system. All of the new initiatives would be funded at the same level throughout the budget period. For example, 2021 initiatives would receive \$500 million each year from 2021 to 2030, 2022 initiatives would receive \$500 million from 2022 to 2030, and so forth.

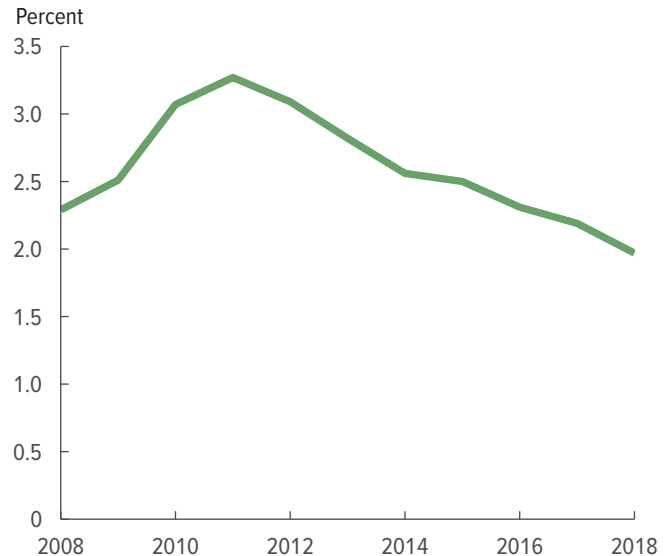
CBO estimates that revenues would increase gradually over the 10-year period, reaching roughly \$9 billion a

39. Other researchers have argued that increasing the audit rates in 2018 to the same levels as in 2011 would have raised \$14 billion in revenues in 2018 and that dedicating additional audit resources only to higher-income taxpayers would have resulted in more revenues. See Natasha Sarin and Lawrence H. Summers, "Shrinking the Tax Gap: Approaches and Revenue Potential," *Tax Notes* (November 18, 2019), <https://tinyurl.com/yd4y5s76>.

40. Funding would be directed to the appropriations accounts for enforcement and operating support to cover increases in costs for agencywide infrastructure, such as offices and computer hardware, for new employees.

Figure 14.

Cases Using Automated Underreporter Software as a Share of Individual Returns



The Internal Revenue Service has reduced its use of the Automated Underreporter program to help analyze returns with discrepancies. The number of cases fell as the number of employees who review those discrepancies and correspond with taxpayers declined by 40 percent between 2010 and 2018.

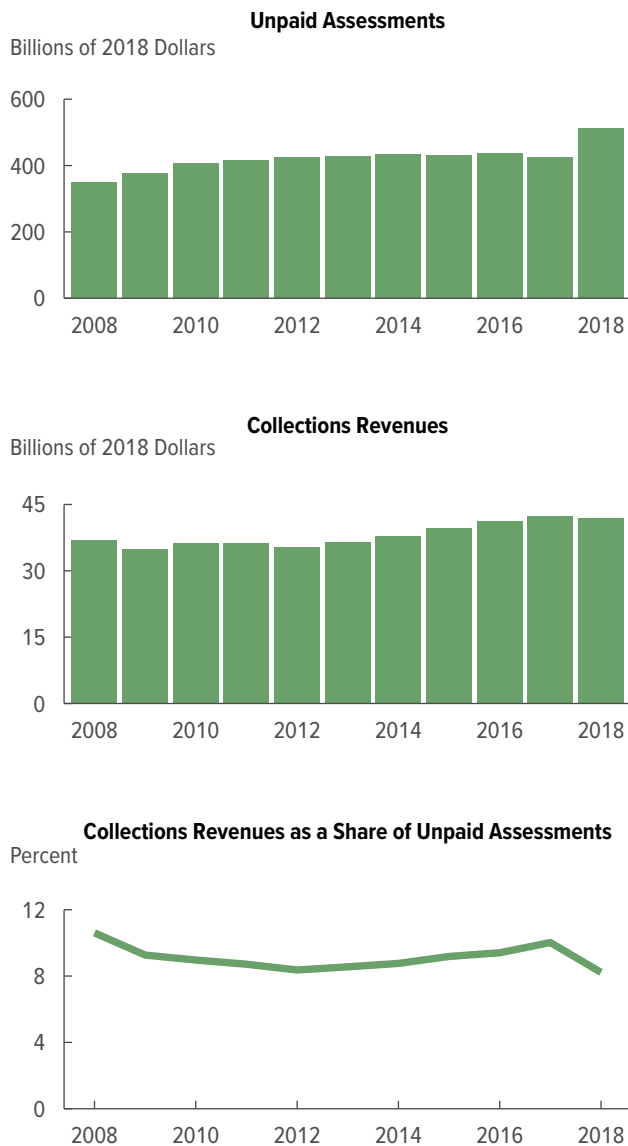
Source: Congressional Budget Office, using data from the Internal Revenue Service.

Cases are measured as the number of examinations closed in a fiscal year. Returns are measured in the fiscal year they were filed.

year from 2027 through 2030. The agency's assessment is based on the amount of time it generally takes new hires to be fully effective. In the first year of an initiative, the return in tax revenue per dollar of spending would be low because new employees need to be hired and trained. The return on the initiative would increase as employees finished their training and gained experience, and it would reach its maximum level in the third year of funding.

Although CBO's estimates start with the IRS's calculations of the revenue it would collect per dollar of enforcement spending, CBO made two adjustments to better approximate the marginal return on that spending. The first is an adjustment for taxpayers' learning. After the third year of an initiative, CBO judges that taxpayers

Figure 15.

Unpaid Assessments and Collections Revenues

Although revenues from collection efforts grew from 2008 to 2018, the amount of uncollected revenues from unpaid assessments grew faster.

Source: Congressional Budget Office, using data from the Internal Revenue Service and the Treasury Inspector General for Tax Administration.

Unpaid assessments are the taxes, penalties, and interest owed to the Internal Revenue Service that fall within the 10-year statute of limitations. Collections revenues are the amount of assessed tax, penalties, and interest that is paid as a result of collections activity.

will have adapted to a new enforcement activity and developed ways to evade that enforcement. CBO therefore reduced the marginal return on each activity after the third year. The second adjustment incorporates the expectation that the IRS prioritizes enforcement activities that it projects to have the highest average return; therefore, the spending associated with the 2021 initiative would have the greatest return, and initiatives that start in the 2022–2025 period would have progressively lower returns.

The return from a particular initiative reflects the amount of revenue that will be collected from it over the next 10 years. CBO converted that return into a stream of revenue receipts on the basis of information from the IRS. Enforcement initiatives that start after 2021 would bring in some revenue outside the 10-year period; CBO's estimate does not include that revenue.

Estimated Revenue Effects of a \$40 Billion Increase.

If the IRS was given twice as much additional funding for enforcement activities as was provided in the first option, CBO estimates that the return per dollar of spending would be less than twice as high, reflecting the expectation that the IRS would focus first on initiatives that generate the most revenue. A \$40 billion increase in the IRS's appropriations would thus boost revenues by \$103 billion if directed to enforcement activities over that period. On net, the increase in the enforcement budget would reduce the deficit by \$63 billion through 2030.

The pattern of funding for the \$40 billion option would follow the previous option, beginning with \$1 billion in additional funds the first year, increasing gradually by \$1 billion per year for the first four years, and then remaining at \$5 billion per year from 2026 to 2030. The adjustment to returns for taxpayer learning would also be the same. But the adjustment for reduced marginal returns would be even larger with each successive initiative because the activities with the highest average return would be undertaken even more quickly than under the first option. Additionally, hiring enough qualified new enforcement employees each year would become more difficult, and training less-qualified employees might involve more time and spending. The amount of added revenues would peak at close to \$15 billion in 2028.

Scorekeeping Guidelines for Formal Cost Estimates

The revenue changes attributable to the two options for increasing enforcement would not be counted in formal cost estimates. Under the Congressional scorekeeping guidelines that govern the cost estimates CBO produces, added revenues or reductions in mandatory spending that might result from additional spending are not included. The Congress established those guidelines in large part to avoid crediting uncertain potential savings as an offset against certain upfront spending. The scorekeeping guidelines were included in the conference report for the Balanced Budget Act of 1997, which aimed to ensure consistent treatment of spending authority, appropriations, and outlays over time.⁴¹ The guidelines were last updated in 2015.

Two guidelines are especially relevant to estimates for legislation that involves enforcement of tax laws. Scorekeeping guideline 3 states: “Revenues, entitlements and other mandatory programs (including offsetting receipts) will be scored at current law levels . . . unless Congressional action modifies the authorizing legislation.” Put another way, potential revenues from legislation will be counted in a cost estimate only if those revenues result from changes in the tax code. Even though additional discretionary appropriations for IRS enforcement may produce budgetary savings (from increased federal tax receipts), such savings are not counted in a cost estimate.

Scorekeeping guideline 14 states: “No increase in receipts or decrease in direct spending will be scored as a result of provisions of a law that provides direct spending for administrative or program management activities.” That guideline prohibits budgetary savings from being counted if they result from funding in authorizing legislation for administrative or program management activities, including increased IRS enforcement.⁴²

How Enforcement Spending Is Reflected in Baseline Revenue Projections

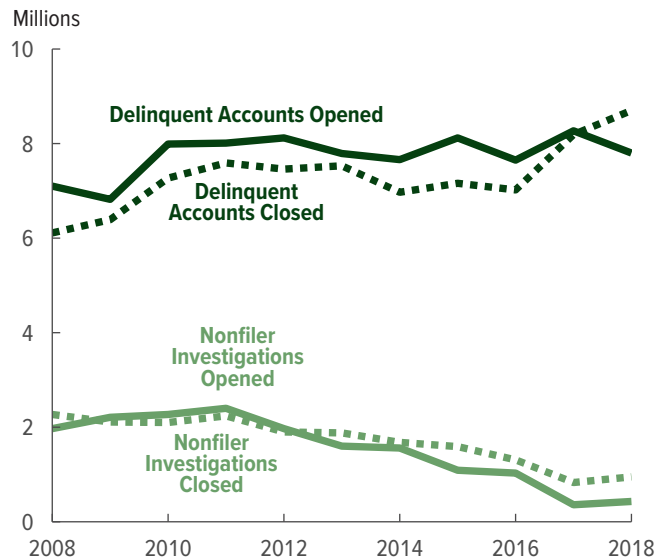
The scorekeeping guidelines do not apply to CBO’s baseline budget projections or to its other projections such as the analysis of the President’s budget. So, although CBO

41. See U.S. House of Representatives, *Balanced Budget Act of 1997: Conference Report to Accompany H.R. 2155*, House Report 105-217 (July 30, 1997), pp. 1007–1014, <https://go.usa.gov/xw7FH> (PDF, 3.2 MB).

42. Funding for the IRS is generally provided through appropriation acts, not authorizing legislation.

Figure 16.

Number of Collections Cases



The Internal Revenue Service’s investigations of people who failed to file returns have declined, as has the number of delinquent accounts it has closed. In 2018, the number of closed accounts increased as the agency transferred some accounts to private collection agencies.

Source: Congressional Budget Office, using data from the Internal Revenue Service.

Delinquent accounts are opened when the Internal Revenue Service determines that taxpayers owe more taxes than they paid. Nonfiler investigations are opened for taxpayers that have not filed a return.

does not include the revenue effects of changes in the IRS’s funding in cost estimates, the agency incorporates both the spending and revenue effects of enacted legislation in its next update of baseline budget projections.

CBO also adjusts baseline projections of revenues from taxes paid on a liability from a prior year, called back taxes, to account for increases or decreases in the real amounts appropriated for enforcement of tax laws. In general, revenues from back taxes are projected on the basis of the historical relationship between those revenues and overall tax liabilities. If the IRS’s resources for enforcement activities in future years are projected to be less than in the past, the expected ratio of revenues from back taxes to overall tax liabilities is lowered.⁴³ (Similarly,

43. In its baseline, CBO projects that individual discretionary appropriations, including those for enforcement activities, grows with inflation; hence, in real dollars, projected funding in all future years is equal to funding for the enforcement account in the most recent appropriation act.

Box 3.

Options for Increasing Tax Revenues

In addition to changing the amount of appropriations for the Internal Revenue Service (IRS) to increase the amount of traditional enforcement activity, policymakers have other options to affect the amount of revenues the IRS brings in under the current tax regime.

In recent testimony to the Congress, the Government Accountability Office (GAO) described many potential changes that could reduce noncompliance with tax laws.¹ A full analysis of those policies is outside the scope of this report, but in brief, GAO suggests that the IRS could do the following:

- Develop a strategy that uses data from its National Research Program (NRP) to update its compliance programs,
- Establish a quantitative goal for improving voluntary compliance,
- Analyze and use results of employment tax NRP examinations to improve employment tax compliance programs, and
- Make greater use of the automated Return Review Program to reduce fraud.

1. See Testimony of James R. McTigue Jr., Director, Strategic Issues, Government Accountability Office, before the House Committee on Ways and Means, *Tax Gap: Multiple Strategies Are Needed to Reduce Noncompliance*, GAO-19-558T (May 9, 2019), www.gao.gov/products/GAO-19-558T.

The tax gap (the difference between taxes owed and taxes paid) could also be reduced if policymakers increased the amount of information available to the IRS or expanded its authority by doing one or more of the following:

- Expanding third-party information reporting to cover more transactions,
- Requiring more taxpayers to electronically file tax and information returns,
- Expanding the IRS's math error authority to other types of discrepancies on tax returns, and
- Giving the IRS the authority to regulate paid tax preparers.

Former IRS Commissioner Charles Rossotti proposed new reporting requirements for small- and medium-sized businesses and also suggested significantly increasing the agency's technology spending to allow wider use of data analysis in fraud detection and enforcement activity (for example, enabling the IRS to automatically generate notices with information specific to each taxpayer).² Those more ambitious proposals to reduce the tax gap would, in the judgment of the Congressional Budget Office, require additional statutory authority (for example, greater information reporting to the IRS) or more fundamental overhauls of the IRS's existing information technology, audit, and enforcement functions.

2. See Charles Rossotti, "Recover \$1.6 Trillion, Modernize Tax Compliance and Assistance," *Tax Notes Federal* (March 2, 2020), p. 1411, <https://tinyurl.com/r7y4jy3>.

that expected ratio would be increased if IRS resources were projected to increase.)

Sources of Uncertainty

Four factors contribute to the uncertainty surrounding the revenue effects of increases in IRS funding. First, although the average return per dollar of enforcement is the best method available to measure the effect of increasing revenues, it is imperfect. Second, the productivity of additional funding would depend on taxpayers' responses to increased enforcement. Third, the effect of additional funding on revenues would depend on

the efficiency with which it was used. Fourth, revenues would be affected by how the IRS chose its caseload.

Use of Average Return per Dollar to Measure

Marginal Returns. Although CBO adjusts the IRS's average-return-per-dollar figure to better measure marginal return, CBO's adjustments may not capture all the ways that changes in the IRS's funding affect revenues (see Appendix B for details on CBO's method for estimating changes in revenues). In particular, the average return per dollar does not incorporate the indirect effects of IRS spending, which are difficult to measure. Excluding the indirect effects of enforcement spending

Table 1.

Estimated Effects of Two Options to Increase Appropriations for the Internal Revenue Service

Billions of Dollars

	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	Total, 2021– 2030
Option 1: Increase Appropriations by \$20 Billion											
Change in Outlays	0.5	1.0	1.5	2.0	2.5	2.5	2.5	2.5	2.5	2.5	20.0
Change in Revenues	0.3	1.5	3.3	5.1	6.8	8.1	8.8	9.0	8.9	8.8	60.6
Increase or Decrease (-) in the Deficit	0.2	-0.5	-1.8	-3.1	-4.3	-5.6	-6.3	-6.5	-6.4	-6.3	-40.6
Option 2: Increase Appropriations by \$40 Billion											
Change in Outlays	1.0	2.0	3.0	4.0	5.0	5.0	5.0	5.0	5.0	5.0	40.0
Change in Revenues	0.7	3.0	6.3	9.4	11.9	13.7	14.6	14.8	14.7	14.4	103.1
Increase or Decrease (-) in the Deficit	0.3	-1.0	-3.3	-5.4	-6.9	-8.7	-9.6	-9.8	-9.7	-9.4	-63.1

Source: Congressional Budget Office.

The effects are calculated based on the assumption that one or both options would take effect in October 2020. Revenues are calculated on the basis of the baseline budget projections that CBO published on March 19, 2020.

may understate the amount of revenue brought in as a result of greater enforcement.⁴⁴

Further complicating the calculation of indirect effects is the fact that enforcement activities with relatively low returns on spending may substantially affect taxpayers' behavior. For example, the ASFR program for nonfilers has a low return on spending because the substitute returns tend to overstate the amount of taxes owed. IRS employees may need to correct the substitute returns (increasing the cost of the program), and they typically reduce the amount due (lowering the program's impact on revenues). However, researchers judge that the program has had a large indirect impact by motivating nonfilers who were affected by the program to file returns in subsequent years.⁴⁵

44. The Treasury Department suggests that the indirect effect of deterrence on revenues is at least three times the direct effect. See Department of the Treasury, "Internal Revenue Service: Program Summary by Appropriations Account and Budget Activity," *Fiscal Year 2017 Budget in Brief*, p. 15, <https://go.usa.gov/xwvzMM> (PDF, 1.95 MB).

45. See Saurabh Datta, Stacy Orlett, and Alex Turk, "Individual Nonfilers and IRS-Generated Tax Assessments: Revenue and Compliance Impacts of IRS Substitute Assessments When Taxpayers Don't File" (paper presented at the IRS–Tax Policy

Taxpayers' Behavior. The returns on additional funding depend on taxpayers' future behavior, including their responses to changes in tax laws and the nature of their employment. If more income was earned in sectors with less third-party reporting—for example, if more taxpayers were self-employed—more IRS resources would be needed to detect the likely uptick in unreported income.

The ways in which taxpayers interact with the IRS and the processes used by the agency also affect the results of enforcement activities. For example, tax returns that are filed on paper must be manually transcribed into the IRS's electronic databases. That process is costly, and transcription errors can be introduced. In addition, only some of the information on a paper return is transcribed, which limits the amount of information available for enforcement activities.⁴⁶ The continued increase in electronic filing and potential changes in how paper returns are processed (for example, by using optical character

Center Research Conference on Tax Administration, Washington, D.C., June 18, 2015), <https://go.usa.gov/xdHTP>.

46. Government Accountability Office, *Tax Fraud and Noncompliance: IRS Could Further Leverage the Return Review Program to Strengthen Tax Enforcement*, GAO-18-544 (July 24, 2018), p. 23, www.gao.gov/products/GAO-18-544.

recognition technology or scannable barcodes) will affect the productivity of the IRS's enforcement programs.

The IRS's reliance on processes such as automated math error correction and partially automated discrepancy review under AUR can also affect revenues if taxpayers do not understand the IRS's notices and cannot provide adequate responses. In both automated processes, taxpayers' ability to appeal an error is more limited than it would be in a traditional examination.

Use of Additional Funding. The steep decline in the IRS's funding after 2010 resulted in substantial staffing reductions. The return on additional funding would depend on the efficiency with which funding can be used—that is, the speed with which the IRS can hire and train new staff and allocate new employees to enforcement activities.

It is uncertain how long it would take for new hires to become productive. The IRS would not be able to bring new hires up to speed instantly, nor is it likely that the agency could hire them quickly. The Government Accountability Office reports that it can take a year or longer from the time an IRS supervisor notifies the division of a staffing need until the employee is on board.⁴⁷ Enforcement staff need to develop specialized expertise to become effective, and the IRS estimates that it can take four to five years to train new hires to become experienced senior-level revenue officers.⁴⁸ In addition, a growing share of the IRS's staff members are eligible for retirement, particularly those in the Senior Executive Service, the federal government's managerial branch.⁴⁹

47. See Government Accountability Office, *Internal Revenue Service: Strategic Human Capital Management Is Needed to Address Serious Risks to IRS's Mission*, GAO-19-176 (March 26, 2019), www.gao.gov/products/GAO-19-176.

48. Ibid.

49. Ibid, Figure 2.

Some of the IRS's activities depend on where its employees are located. Correspondence audits and other routine enforcement functions are conducted from campuses around the country. Work that involves face-to-face contact with taxpayers, such as field audits and field collections, is conducted from local IRS offices. For those activities, the effectiveness of additional employees would depend on those employees' location.

Choice of Cases for Examination. CBO's revenue estimates incorporate the expectation that the IRS would choose to work the cases with the highest return first. But the IRS might choose a different mix of cases to meet other goals, such as balancing enforcement among different types of taxpayers. For example, the average return on correspondence cases is substantially higher than the average return on field examinations, even though correspondence cases bring in less revenue, on average.⁵⁰ That is because field examinations are substantially more costly: They require experienced employees and take more time to complete. However, the IRS might choose to conduct more field examinations, which typically involve corporations or other taxpayers with business income, to ensure that those taxpayers comply with tax laws. Moreover, because different types of tax issues require examiners with different skills and levels of expertise, the IRS's ability to change the types of cases it pursues is limited by the number of employees that have particular skills.⁵¹

50. See Janet Holtzblatt and Jamie McGuire, "Effects of Recent Reductions in the Internal Revenue Service's Appropriations on Revenues" *IRS Research Bulletin*, Publication 1500 (June 2020), www.irs.gov/pub/irs-pdf/p1500.pdf#page=134 (PDF, 9 MB).

51. See Charles P. Rettig, IRS Commissioner, letter to the Honorable Ron Wyden, Ranking Member, Senate Finance Committee (September 6, 2019), <https://go.usa.gov/xfawP>.



Appendix A: Detailed View of Tax Law Enforcement

The Internal Revenue Service (IRS) uses a variety of approaches to prevent fraud, determine the correct amount of taxes owed, collect taxes that were not paid, and secure returns that were not filed. Automated enforcement efforts are used to screen for fraud and to determine tax liability when returns have arithmetic or clerical errors or conflict with third-party information. Examinations are used to determine liability for more complex return issues. For unpaid debts or unfiled returns, the IRS alerts taxpayers and seeks to collect payments on a filed return.

Automated Enforcement Efforts

The IRS uses several software programs that rely on computer models to flag suspicious returns or to correct a return without a formal examination.

Fraud Detection

The IRS suspends the processing of refunds for taxpayers with questionable income tax returns using two fraud detection systems: the Dependent Database and the Return Review Program. The Dependent Database combines information from the Department of Health and Human Services and the Social Security Administration that could establish a relationship between a dependent and taxpayer. The IRS checks return information against those data and applies rules to identify those returns that may have been submitted by an identity thief using another person's name and taxpayer identification number to file a fraudulent return or obtain a fraudulent tax refund.¹

The Return Review Program uses third-party information returns, the taxpayer's previous returns, and several

analytical methods to produce a score that reflects the likelihood of both identify-theft fraud and refund-related fraud such as inflating the amount of wage or self-employment income to receive a larger earned income tax credit (EITC).² For returns with markers of potential identity theft, taxpayers must contact the IRS to verify their identity. For returns with markers of potential refund-related fraud, tax examiners review and verify income and withholding information on the return.

Correction of Mathematical and Clerical Errors

The IRS is authorized by law to correct certain mathematical or clerical errors (collectively referred to as math errors) on a tax return and issue a notice to the taxpayer with the new assessment, including any applicable penalties. Such errors include using the wrong entry from a table or schedule, omitting a form needed to substantiate an entry, claiming a deduction or credit in excess of the statutory limit, and omitting Social Security numbers or taxpayer identification numbers.³

Math errors that the IRS is authorized to correct are identified and corrected immediately when a tax return is processed by the IRS. A notice is sent to the taxpayer with an explanation of the error and the correction, which could be favorable to the taxpayer (resulting in a smaller balance due or a larger refund) or unfavorable (resulting in an additional tax or smaller refund). The taxpayer has 60 days from the date of the math error notice to challenge the correction. Corrected refund amounts are paid to the taxpayer within two to three weeks of the notice, regardless of whether the correction is challenged. If the correction is not challenged, any additional tax is due 60 days from the date of the notice, and the corrected refund amount already issued becomes final.

1. The IRS views the Dependent Database and the Return Review Program as complementary detection systems for identity theft fraud. See Treasury Inspector General for Tax Administration, *The Return Review Program Increases Fraud Detection; However, Full Retirement of the Electronic Fraud Detection System Will Be Delayed*, Reference Number 2017-20-080 (September 25, 2017), <https://go.usa.gov/xdH4a> (PDF, 336 KB). The Dependent Database is also used to select individual returns with refundable credits for examination, which occurs after the fraud detection process. See *Case 3:21-cv-00419 Document 49-2 Filed 03/14/22 Page 220 of 465 PageID #: 376*

2. For more information about the Return Review Program, see Government Accountability Office, *Tax Fraud and Noncompliance: IRS Could Further Leverage the Return Review Program to Strengthen Tax Enforcement*, GAO-18-544 (July 24, 2018), www.gao.gov/products/GAO-18-544.

3. See 26 U.S.C. §6213(g)(2) for a complete list of mathematical and clerical errors.

Comparison of Returns With Information From Third Parties

After returns have been processed, the IRS matches third-party information returns, which provide information on the amounts paid to or processed for the taxpayer, against the processed returns and selects a portion of returns with discrepancies for the Automated Underreporter program (AUR). The AUR's process is similar to the process for a correspondence examination. Taxpayers whose returns have been updated with third-party information are notified of the change and any additional tax, penalties, or interest.⁴ For example, if wages shown on a Form W-2 are greater than the amount of wages reported on the return, the taxpayer is notified that he or she owes additional tax based on the income shown on the W-2. The taxpayer can submit documentation to verify the amount on the return or accept the change and pay the additional tax.

If the taxpayer does not respond to the notice or does not have documentation that resolves the discrepancy, the IRS sends a notice of its intention to assess any additional tax due, known as a statutory notice of deficiency. That notice gives the taxpayer 90 days (150 days if the taxpayer does not reside in the United States) to petition the Tax Court if he or she would like to challenge the AUR results without paying the recommended additional tax. Otherwise, the IRS assesses the additional tax at the end of the 90-day or 150-day period.

Comparisons between processed returns and third-party information returns are made three times a year. For a return filed by April 15, the IRS performs the first match in July and begins notifying taxpayers of discrepancies in late October. In calendar year 2011, on average, 13 months elapsed between filing and notification of a discrepancy.⁵

4. The AUR program automatically applies accuracy-related penalties in cases of substantial understating of income. An examiner evaluates whether the taxpayer had reasonable cause for understatement and, if so, can waive the automatic penalty. See Treasury Inspector General for Tax Administration, *Automated Underreporter Program Tax Assessments Have Increased Significantly; However, Accuracy-Related Penalties Were Not Always Assessed When Warranted*, Reference Number 2015-30-037 (May 8, 2015), <https://go.usa.gov/xdHTtr>.

5. See Government Accountability Office, *Tax Refunds: IRS Is Exploring Verification Improvements, but Needs to Better Manage Risks*, GAO-13-515 (June 4, 2013), Figure 5, www.gao.gov/products/GAO-13-515.

Examinations

Examinations, or audits, which can require a substantial amount of employees' time, are undertaken for some returns. Examinations can be conducted by correspondence or in person, depending on the type of taxpayer and the complexity of the case. Typically, the IRS has up to three years from the date a return was due or filed to assess additional tax.

Identifying Cases

The IRS creates an inventory of returns that have audit potential. There are many ways a return can be selected to be included in that pool, which vary by type of return and by the IRS unit that would conduct the audit. Some mechanisms for selection common to all types of income tax returns are the following:

Computer Screening. Computer algorithms score the likelihood of noncompliance on individual and corporate income tax returns. The Discriminant Inventory Function (DIF) system is used on individual returns and corporate returns of entities with assets of less than \$10 million, and the Discriminant Analysis System (DAS) is used for larger corporate returns.⁶ On the basis of existing data, formulas are developed that assign weights to certain characteristics of returns.⁷ The score derived from the weights is used to rank returns, with a higher score indicating a higher probability of an examination generating a significant tax change. Returns with high DIF or DAS scores are screened by tax examiners, and some are selected for examination.

Data Discrepancies. Discrepancies between information provided to the IRS by third parties (such as states,

6. The Small Business/Self-Employed Division examines corporate returns of entities with assets of less than \$10 million and individual returns that do not claim refundable credits. About 20 percent of examinations closed by the division in 2014 were selected for examination because of the return's DIF score. See Government Accountability Office, *IRS Return Selection: Certain Internal Controls for Audits in the Small Business and Self-Employed Division Should Be Strengthened*, GAO-16-103 (December 16, 2015), Figure 3, www.gao.gov/products/GAO-16-103. DAS is the main selection method of the Large Business and International Division, which examines corporate returns with assets of more than \$10 million. See Government Accountability Office, *IRS Return Selection: Improved Planning, Internal Controls, and Data Would Enhance Large Business Division Efforts to Implement New Compliance Approach*, GAO-17-324 (March 28, 2017), www.gao.gov/products/GAO-17-324.
7. Compliance data collected by the National Research Program from examinations are used to improve the DIF algorithm.

employers, banks, payment processors, brokers, or other federal agencies) on income or dependents claimed on the return can prompt a screening of a return for potential audit.⁸

Focus Area. In the case of large and international businesses, a return may be selected for examination because it has characteristics that match an issue-based area of focus, called a “campaign.” Campaigns identify narrow issues that represent a high risk of noncompliance and select returns with those issues for audit or for notices intended to educate the taxpayer. Such campaigns may focus, for example, on taxpayers who claim an individual foreign tax credit but do not meet the requirements, taxpayers with offshore private bank accounts, or taxpayers that claim a property deduction for an energy-efficient commercial building.⁹ The IRS also periodically identifies abusive tax avoidance schemes as areas of focus, such as syndicated conservation easements, in which investors claim a deduction for a charitable contribution based on an inflated value for the conservation easement.

Related Returns. When an examination is opened, prior or subsequent returns filed by the taxpayer, or returns filed by related taxpayers like business partners, may also be selected for examination.

Referrals. Taxpayers suspected of noncompliance can be referred for IRS examination by federal, state, or local government agencies, or by citizen whistleblowers.¹⁰ Other IRS programs can also refer suspicious returns for examination.

Mandatory Review. Certain types of returns are always examined because of law or IRS policy. For example, the IRS examines all returns that claim a refund of more than \$2 million (or \$5 million for C corporations) and submits a report to the Joint Committee on Taxation.¹¹ Other returns that are routinely examined include those of certain IRS employees, the President, and the Vice President. Examiners also review amended returns, which must be manually processed.

Random Selection. The IRS's National Research Program (NRP) selects a random sample of returns for examination to provide the agency with information about voluntary compliance. Though the primary purpose of NRP examinations is to gather statistically valid data on compliance that are used in estimating the tax gap and informing computer screening for audit, corrections made as information on a return is verified can result in recommended additional tax for the taxpayer, just as it would in an operational (non-NRP) examination. The NRP's main study is an annual sample of individual income tax returns (Form 1040), which it has conducted since the program was started in 2000.¹² The NRP has also conducted two smaller studies—a sample of S corporation tax returns (Form 1120-S) from tax years 2003 and 2004, and a sample of employment tax returns (Form 941) from tax years 2008 to 2010.

Examination Process

When an auditor receives a case for examination, he or she identifies issues on the return that could change tax liability. Managers then order examinations on the basis of available staff, funding and the IRS's enforcement priorities.

Types of Examinations

Returns with issues that could be resolved with a limited amount of additional documentation from the taxpayer are conducted entirely through correspondence. Those examinations typically involve individual returns with claims for EITC or other refundable credits, itemized

8. The Wage and Investment Division examines individual returns claiming refundable credits. In 2014, 59 percent of that division's examinations were selected using the Dependent Database, which uses internal IRS data as well as external data on child custody from the Department of Health and Human Services and birth information from the Social Security Administration to identify discrepancies on returns. See Government Accountability Office, *IRS Return Selection: Wage and Investment Division Should Define Audit Objectives and Refine Other Internal Controls*, GAO-16-102 (December 17, 2015), www.gao.gov/products/GAO-16-102.

9. Since January 2017, the Large Business and International Division has introduced a total of 53 compliance campaigns that guide the selection of returns for audit. For a list of all of the division's active and retired campaigns, see Internal Revenue Service, “Large Business and International Compliance Campaigns” (accessed June 17, 2020), <https://go.usa.gov/xdspdy>.

10. See Internal Revenue Service, *Publication 556: Examination of Returns, Appeal Rights, and Claims for Refund* (September 2013), www.irs.gov/pub/irs-pdf/p556.pdf (1.2 MB).

11. See Joint Committee on Taxation, “Joint Committee Statutory Refund Review” (accessed June 17, 2020), www.jct.gov/about-us/refund-review.html.

12. Since 2007, the National Research Program's individual compliance study has combined examination results from a rolling three-year period, with annual sample sizes of about 13,000 returns. Previously, this study selected about 45,000 returns from a single tax year. See Internal Revenue Service, “IRS Updates National Research Program for Individuals,” IR-2007-113 (news release, June 6, 2007), www.irs.gov/pub/irs-news/ir-07-113.pdf (19 KB).

deductions, or expenses related to self-employment income. A correspondence examination begins with a notice letter, informing the taxpayer that his or her return is under examination and listing documentation the taxpayer needs to provide to resolve the issue. A taxpayer has 30 days to respond to a notice letter with supporting documents or to request a 30-day extension, which is ordinarily granted. The scope of a correspondence examination can expand if the auditor identifies additional issues in the return, but it is typically limited to verifying lines in the return that are related to the issue that prompted the audit.¹³ Correspondence examinations accounted for 81 percent of individual income tax examinations and 2 percent of corporate income tax examinations in 2018.

When an examination involves more complicated issues, it requires an in-person meeting between an IRS employee and the taxpayer to review records and allow the taxpayer to provide oral testimony. The meeting may take place at an IRS office, for examinations of limited complexity; more complex examinations may occur “in the field,” at the taxpayer’s home or business.¹⁴

If the information a taxpayer provides during a correspondence, office, or field examination is sufficient to resolve all issues, the IRS accepts the original return as filed with no additional tax assessed. If not, the IRS proposes changes to the return in a letter with an audit report. Examiners are responsible for recommending additional tax and for adding civil penalties if applicable.¹⁵ The taxpayer has 30 days to agree to any recommended additional tax and penalties

or to challenge the assessment through the independent appeals function of the IRS.

If the taxpayer does not agree to the audit report or appeal its findings within 30 days, the IRS sends a statutory notice of deficiency. That notice gives the taxpayer 90 days (or 150 days if the taxpayer does not reside in the United States) to petition the Tax Court if he or she would like to challenge the examination results without paying the recommended additional tax. Otherwise, the IRS assesses the additional tax at the end of the 90-day or 150-day period.

The length of time it takes to complete an examination varies by the examination and taxpayer type. On average, in 2014, an audit took about 270 days between when a return was filed and when an examination was closed.¹⁶ Among taxpayers who have self-employment income or are small businesses, field audits took an average of 310 days in 2014, whereas office audits took an average of 262 days. Correspondence audits of individuals and small businesses were generally shorter; in the 2017–2018 period, they averaged 190 days for individuals and 229 days for small businesses, with refunds sometimes frozen during that time.¹⁷ The length of audits of large corporations ranged, on average, between 29 months and 48 months, in 2012.¹⁸ Refunds are generally not frozen for field or office audits.

Collections

The IRS collects unpaid taxes and secures tax returns that have not been filed. The agency has the authority to place liens on a taxpayer’s property or seize their property to satisfy a tax debt (including garnishing wages from

13. See Government Accountability Office, *IRS Correspondence Audits: Better Management Could Improve Tax Compliance and Reduce Taxpayer Burden*, GAO-14-479 (June 5, 2014), www.gao.gov/products/GAO-14-479.

14. The amount of time allotted for an audit by a tax compliance officer is much shorter than the amount allotted for an audit by a revenue agent because tax compliance officers address less complicated issues. See National Taxpayer Advocate, “Office Examination: The IRS Does Not Know Whether Its Office Examination Program Increases Voluntary Compliance or Educates the Audited Taxpayers About How to Comply in the Future,” *Annual Report to Congress 2018* (February 2019), vol. 1, pp. 153–163, <https://taxpayeradvocate.irs.gov/2018AnnualReport>.

15. For example, if an individual taxpayer underreported income and the recommended additional tax from examination of his or her return is greater than \$5,000, the taxpayer may be assessed a penalty of 20 percent of the recommended additional tax for substantially understating income. In 2018, \$1.5 billion in accuracy-related penalties was assessed on individual tax returns (from any tax year), and \$0.2 billion in accuracy-related penalties was assessed on corporate tax returns. See Internal Revenue

Service, *Internal Revenue Service Data Book, 2018* (June 30, 2020), <https://go.usa.gov/xfcy3>.

16. See Government Accountability Office, *IRS Return Selection: Certain Internal Controls for Audits in the Small Business and Self-Employed Division Should Be Strengthened*, GAO-16-103 (December 16, 2015), Table 3, www.gao.gov/products/GAO-16-103.

17. See National Taxpayer Advocate, “Correspondence Examinations: The IRS’s Correspondence Examination Procedures Burden Taxpayers and Are Not Effective in Educating the Taxpayer and Promoting Future Voluntary Compliance,” *Annual Report to Congress 2018* (February 2019), vol. 1, pp. 126–141, <https://taxpayeradvocate.irs.gov/2018AnnualReport>.

18. See Government Accountability Office, *Corporate Tax Compliance: IRS Should Determine Whether Its Streamlined Corporate Audit Process Is Meeting Its Goals*, GAO-13-662 (August 2013), Figure 1, www.gao.gov/products/GAO-13-662.

employers). Typically, the IRS has up to 10 years from the date taxes were assessed to collect them.

Identifying Cases

Collections cases can originate from returns that did not include full payment of taxes, assessments resulting from examinations or automated enforcement efforts that are not paid promptly, and IRS programs that identify nonfilers based on third-party information returns.

Collections Process

Because of limited resources and the vast pool of potential cases, the IRS prioritizes resolving cases quickly and at the lowest cost. It first sends a number of computer-generated notices to the taxpayer about the unpaid tax or delinquent return before using more labor-intensive methods. Taxpayers who file a return but do not pay the full amount of tax due receive up to four notices over 20 weeks; individual income tax nonfilers receive up to two notices and have 14 weeks to respond.¹⁹

For cases that remain unresolved after the initial notice phase, the IRS may open a taxpayer delinquent account (for a return that was filed with inadequate payment) or a taxpayer delinquent investigation (for an unfiled return). Cases are then assigned to different collection processes depending on whether they are likely to be collectible, the amount and type of tax owed, and the age of the account. Interest and penalties accrue until the debt is paid in full.²⁰ Within each process, an automated system ranks cases so that higher-priority cases are handled first. Cases can also be shuffled between the various processes described below.

19. For more information on the collections process for individual income tax nonfilers, see Saurabh Datta, Stacy Orlett, and Alex Turk, "Individual Nonfilers and IRS-Generated Tax Assessments: Revenue and Compliance Impacts of IRS Substitute Assessments When Taxpayers Don't File" (paper presented at the IRS–Tax Policy Center (TPC) Research Conference, Washington, D.C., June 18, 2015), <https://go.usa.gov/xdHTP>.

20. Unpaid tax debt is subject to penalties and interest. Interest accrues on any unpaid tax from the date the return is due until the date of full payment, at the interest rate on federal short-term debt plus 3 percent. Penalties for failure to file or failure to pay are calculated as a percentage of the tax due, and grow each month that the return remains unfiled or the tax debt unpaid. See Internal Revenue Service, "Topic No. 653: IRS Notices and Bills, Penalties, and Interest Charges" (July 1, 2020), www.irs.gov/taxtopics/tc653.

- IRS representatives in the Automated Collection System (ACS) make telephone contact with taxpayers and issue notices of federal tax liens and levies.
- In field collection, a revenue officer makes in-person contact with the taxpayer. Managers assign cases based on the characteristics of the revenue officer, including geographic proximity and expertise, and characteristics of the case, such as its potential for collectability.
- Cases that are awaiting assignment to a revenue officer for field collection or to the ACS are held in a queue.
- Cases that are predicted to be unproductive or have not been assigned after being in the queue for a year are put on hold, or shelved. The IRS typically does not further pursue shelved cases unless the taxpayer has additional tax debts or delinquent returns, or unless penalties and interest accruing on the shelved case become sufficiently large that the case is moved back into active collection. Some shelved cases are transferred to private collection agencies (see next section).
- Some cases involving taxpayers who did not file a required return are assigned to the Automated Substitute for Return program. For those cases, the IRS creates a return based on income reported on information returns. The assessed tax is calculated on the assumption that the taxpayer's status is either single or married filing separately (if the taxpayer previously filed as married) and that he or she claims the standard deduction.²¹ That proposed tax liability may be higher than the taxpayer's actual tax liability would have been if he or she had filed a return.

A collections case can be resolved in several ways. Taxpayers can pay the full amount owed or apply for an installment payment plan. They can request a reduction of the amount owed (known as an offer in compromise). If a taxpayer is facing financial hardship, the IRS can analyze his or her financial situation and potentially

21. The IRS also includes one personal exemption in calculating tax liability on a substitute return. However, the 2017 tax act (Public Law 115-97) temporarily suspended personal exemptions for tax years 2018 to 2025.

suspend active collection of tax debts.²² Otherwise, the IRS may seize a taxpayer's property to satisfy the tax debt or place a federal tax lien on a taxpayer's property. Generally, taxpayers have 30 days to appeal IRS collections actions after receiving a notice. Following the appeals determination, the taxpayer has 30 days to contest it in Tax Court.²³

Role of Private Collection Agencies

The Fixing America's Surface Transportation Act of 2015 required that the IRS use private collection agencies (PCAs) to collect unpaid assessments that the IRS is not currently pursuing. Cases that are eligible to be transferred are generally those that the IRS has shelved, those that it did not assign to an employee for collection, or those in which there has been no contact between the IRS and the taxpayer for over a year. Certain cases, such as those involving taxpayers who are under age 18 or who are victims of identity theft, cannot be transferred. The Taxpayer First Act of 2019 further restricted the IRS from transferring the tax debts of low-income taxpayers to PCAs.

PCAs receive a commission of 25 percent of the amount collected, and the IRS can retain another 25 percent of the amount collected to hire and train "special compliance personnel" to work in field collection or in the ACS. The IRS began transferring cases to PCAs in 2017. As of September 2018, PCAs had received responsibility for collecting about \$5.7 billion worth of debt from more than 700,000 taxpayers. The PCAs had collected \$89 million and resolved about 38,000 cases with full payment or with an installment agreement through that time.²⁴ During that period, the IRS paid \$16 million in commissions and spent another \$50 million to

implement and manage the program, resulting in a net gain of \$22 million.

The use of PCAs can allow collection of tax debt the IRS does not have the resources to pursue. Revenue generated from the use of PCAs can be counted in the Congressional Budget Office's cost estimate for legislation authorizing their use, unlike estimates of revenue generated from increased enforcement spending.²⁵ However, previous IRS programs using PCAs in 1996 and from 2006 to 2009 ended because they were not cost effective.²⁶ Cases assigned to PCAs are, on average, almost four years old—but after three years, debts tend to be uncollectible.²⁷ The IRS predicts that those cases would have low returns, and given the agency's limited resources, it is unlikely that the IRS would pursue them.

Some advocates for taxpayers are concerned that the use of PCAs may impose hardships on taxpayers. Although the IRS is required to take into account the taxpayer's ability to pay his or her tax debt, those guidelines do not apply to PCAs, and they do not have the ability to offer alternatives to collection such as an offer in compromise.²⁸ The use of PCAs may also make taxpayers more vulnerable to identity theft if taxpayers cannot distinguish between a phone call from a legitimate PCA or an impersonator.

and Better Protect Taxpayers, GAO-19-193 (March 29, 2019), www.gao.gov/products/GAO-19-193.

22. If the financial analysis shows that a taxpayer's income is not sufficient to provide a minimum standard of living, the IRS places the taxpayer in "currently not collectible" status and does not actively try to collect that person's tax debt. The debt will continue to accrue penalties and interest, and income tax refunds may be used to offset the debt. See Taxpayer Advocate, "Currently Not Collectible" (accessed June 22, 2020), <https://go.usa.gov/xw7Ds>.
23. The appeals process differs by the type of collections action. For more details, see Internal Revenue Service, *Collection Appeal Rights*, Publication 1660 (revised January 2020), www.irs.gov/pub/irs-pdf/p1660.pdf (657 KB).
24. See Government Accountability Office, *Tax Debt Collection Contracts: IRS Analysis Could Help Improve Program Results*

25. See Congressional Budget Office, cost estimate for the conference agreement on H.R. 22, the FAST Act (December 2, 2015), <https://go.usa.gov/xvekz>.
26. The earlier programs differ from the current one in several ways, including the structure of payments to PCAs and the types of cases the IRS transferred to PCAs.
27. See Treasury Inspector General for Tax Administration, *Private Debt Collection Was Implemented Despite Resource Challenges; However, Internal Support and Taxpayer Protections Are Limited*, Reference Number 2018-30-052 (September 5, 2018), <https://go.usa.gov/xw7WR> (PDF, 3.3 MB).
28. See National Taxpayer Advocate, "Private Debt Collection: The IRS's Expanding Private Debt Collection Program Continues to Burden Taxpayers Who Are Likely Experiencing Economic Hardship While Inactive Private Collection Agency Inventory Accumulates," *Annual Report to Congress 2018* (February 2019), vol. 1, pp. 277–294, <https://taxpayeradvocate.irs.gov/2018AnnualReport>.



Appendix B: CBO's Approach to Estimating Changes in Revenues

The Congressional Budget Office estimated the effect of changes in revenues collected by the Internal Revenue Service (IRS) by calculating the amount that revenues would increase for each additional dollar of enforcement spending. The starting point for its projections was the estimates that the IRS typically provides as part of the President's annual set of budgetary proposals. The IRS estimates a return-on-investment (ROI) factor for spending on new enforcement initiatives by calculating the expected revenues that would be raised from taxes, interest, and penalties as a result of the new initiatives divided by their additional cost. That additional cost is based on the cost of the employees required to implement the new initiatives—that is, the pay grade of those employees and the number of hours they work. The IRS's ROI factors have ranged from 5.2 to 9.2 since 2016.

CBO used IRS estimates from multiple years of the President's budget to estimate a general ROI factor equal to 6.4 for broadly increasing the IRS's enforcement funding. CBO anticipates that the return on enforcement would rise to 6.4 over the first three years of an initiative as employees finished training and became more skilled in enforcement. In CBO's assessment, that return would then decline in the later years of a given set of initiatives and for initiatives that start in later years of a funding proposal. The decline reflects CBO's expectation that the

IRS would focus first on the cases that bring in the most potential revenue (the amount of spending times the expected return) and then move to cases that are likely to yield less revenue. In addition, CBO expects that taxpayers would adjust their behavior over time to avoid the new compliance activities. Finally, CBO estimates how much revenue would be collected and when the IRS would receive that revenue.

To illustrate its approach, CBO calculated how spending and revenues would be affected by each new set of initiatives that would result from a \$20 billion increase in the IRS's appropriations over 10 years (See Table B-1). In this illustration, initiatives that begin in 2021 receive \$500 million in funding each year from 2021 to 2030 and generate \$20 billion in revenues over that period. The 2022 initiatives similarly receive \$500 million in funding each year from 2022 to 2030, generating \$15 billion in revenue by 2030. Revenues are lower for each successive set of initiatives because CBO projects that they would focus on lower-yielding enforcement activities and because less of the potential revenue would be collected within the 10-year period. (For example, additional revenues generated by the 2021 initiatives during the first six years are projected to be almost twice the revenues generated by the 2025 initiatives in their first six years.)

Table B-1.

Estimated Effect of Increasing Appropriations for the Internal Revenue Service by \$20 Billion

Billions of Dollars

	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	Total, 2021– 2030
Change in Outlays	0.5	1.0	1.5	2.0	2.5	2.5	2.5	2.5	2.5	2.5	20.0
Change in Revenues											
2021 initiatives	0.3	1.2	2.0	2.3	2.4	2.5	2.4	2.4	2.3	2.3	20.3
2022 initiatives		0.3	1.1	1.7	2.0	2.1	2.1	2.1	2.0	2.0	15.3
2023 initiatives			0.2	0.9	1.5	1.7	1.8	1.8	1.8	1.7	11.3
2024 initiatives				0.2	0.8	1.2	1.4	1.5	1.5	1.5	8.1
2025 initiatives					0.2	0.6	1.1	1.2	1.3	1.3	5.6
Total Change in Revenues	0.3	1.5	3.3	5.1	6.8	8.1	8.8	9.0	8.9	8.8	60.6
Increase or Decrease (-) in the Deficit	0.2	-0.5	-1.8	-3.1	-4.3	-5.6	-6.3	-6.5	-6.4	-6.3	-40.6

Source: Congressional Budget Office.

The option would take effect in October 2020.

Because of the budget scorekeeping guidelines used by the Congress, the revenue changes attributable to this option would not be counted for budget enforcement purposes. However, if an appropriation bill or another bill providing funding for this option was enacted, CBO's next projection of the budget deficit would incorporate its projected effects on revenues.



List of Tables and Figures

Tables

1.	Estimated Effects of Two Options to Increase Appropriations for the Internal Revenue Service	23
B-1.	Estimated Effect of Increasing Appropriations for the Internal Revenue Service by \$20 Billion	32

Figures

1.	Estimated Amount of Unpaid Taxes	3
2.	Unpaid Taxes, by Method of Avoiding Payment	4
3.	Amount of Underreported Tax on Individual Income Tax Returns, by Type of Reporting Error	5
4.	Relationship Between Unpaid Individual Income Taxes and Third-Party Data	6
5.	Overview of Enforcement Activities of the Internal Revenue Service	7
6.	Funding and Number of Employees of the Internal Revenue Service, by Appropriation Account	10
7.	Employees in Selected Enforcement Positions	11
8.	Examination Rate for Individual Returns, by Type of Examination	12
9.	Examination Rate for Individual Returns, by Amount of Income	13
10.	Examination Rate for Certain Returns With and Without the Earned Income Tax Credit	15
11.	Examination Rate for Corporate Returns, by Type of Examination	16
12.	Examination Rate for Corporate Returns, by Amount of Assets	17
13.	Amount of Additional Tax Recommended After Audits	18
14.	Cases Using Automated Underreporter Software as a Share of Individual Returns	19
15.	Unpaid Assessments and Collections Revenues	20
16.	Number of Collections Cases	21



About This Document

This report was prepared at the request of the Ranking Member of the Senate Budget Committee. In keeping with the Congressional Budget Office's mandate to provide objective, impartial analysis, the report makes no recommendations.

Kathleen Burke and Shannon Mok wrote the report, with guidance from Janet Holtzblatt (formerly of CBO), Joseph Rosenberg, and John McClelland. Matthew Pickford provided useful comments. Brian Erard of B. Erard & Associates, Dayanand Manoli of the University of Texas at Austin, and Erin Towery of the University of Georgia also provided helpful comments. The assistance of external reviewers implies no responsibility for the final product, which rests solely with CBO.

Jeffrey Kling, Wendy Edelberg (formerly of CBO), and Robert Sunshine reviewed the report. Elizabeth Schwinn was the editor, and Casey Labrack was the graphics editor. An electronic version is available on CBO's website (www.cbo.gov/publication/56422).

CBO continually seeks feedback to make its work as useful as possible. Please send any comments to communications@cbo.gov.

Phillip L. Swagel
Director
July 2020

IRS Initiates 'Operation Hidden Treasure' to Root Out Unreported Crypto Income

"These transactions are not anonymous," the IRS' national fraud counsel said. "We see you."

By Daniel Kuhn

Mar 7, 2021 at 3:22 p.m. EST

Updated Sep 14, 2021 at 8:22 a.m. EDT



The U.S. Internal Revenue Service (IRS) appears to be stepping up its enforcement capabilities with a new program dedicated to cryptocurrency tax compliance.

With “Operation Hidden Treasure,” the IRS will search for unreported crypto-related income, according to Director of the Office of Fraud Enforcement Damon Rowe.

- Speaking at a Federal Bar Association virtual tax conference, Rowe said cryptocurrency fraud will be a priority. Forbes [first reported](#) the news.
- Operation Hidden Treasure, a joint effort between the IRS’ civil office of fraud enforcement and its criminal investigation unit, will train agents to look at blockchains to root out tax evasion among cryptocurrency users. It will exist as part of the office’s emerging threats mitigation team, Forbes said.
- IRS employees are also reportedly training alongside the European Union Agency for Law Enforcement Cooperation (Europol) as part of the initiative.

Carolyn Schenck, national fraud counsel in the IRS Office of Chief Counsel, told conference-goers the agency is working with private contractors and vendors, presumably blockchain analytics firms, to develop “signatures,” or telltale signs of fraudulent activity.

- These indicators include looking at those who structure transactions just below reporting requirements (like sending a series of \$10,000 transactions), using shell corporations to hide funds as well as “getting on and off the chain,” Schenck reportedly said.
- The IRS has sent conflicting messages to U.S. crypto holders [several times](#) in the past. Most recently, an updated FAQ page indicated that

investors who simply bought “virtual currency with real currency” would not have to report that transaction on this year’s tax returns.

- Still, cashing out crypto or making every-day purchases is typically seen as a taxable event. Operation Hidden Treasure is designed to find, trace, and attribute such transactions to taxpayers, Schenck said.

“These transactions are not anonymous,” she said. “We see you.”

See our research on: [Russia](#) | [Supreme Court](#) | [COVID-19](#)

Pew Research Center

Search [pewresearch.org...](#)[RESEARCH TOPICS](#) ▼ [ALL PUBLICATIONS](#) [METHODS](#) [SHORT READS](#) [TOOLS & RESOURCES](#) [EXPERTS](#) [ABOUT](#)[Home](#) > [Research Topics](#)

MAY 16, 2013



IRS among least-popular federal agencies

BY [DREW DESILVER](#)

The Internal Revenue Service, now under intense scrutiny for [singling out conservative groups](#) seeking tax-exempt status for special review, is one of the least-popular federal agencies — but not quite at the bottom.

In a 2010 Pew Research survey, 47% of people said they had a “very” or “mostly” favorable opinion of the IRS. That was the second-lowest among the 13 agencies people were asked about; only the Department of Education, with a 40% favorability rating, fared worse. Four-in-ten people said they had an unfavorable opinion of the IRS, again exceeded only by the Education Department, with a 53% unfavorability rating.

When people were asked to rate the agencies’ performance, the IRS didn’t fare much better. Only 40% said it was doing an “excellent” (5%) or “good” (35%) job; 38% rated its performance fair and 16% said it was poor.

That put the IRS 11th out of 14 agencies (the 13 mentioned above plus the Homeland Security Department) in terms of public perception of their performance. Ranking lower were the Justice Department (38% excellent or good), the Social Security Administration

Case 3:21-cv-00419 Document 49-2 Filed 03/14/22 Page 233 of 465 PageID #: 389

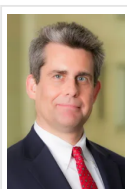
(36%) and the Education Department (33%). Still, all agencies fared better than Congress, which had only 26% favorable rating in 2010; [it's fallen even further](#) since then. [Read more](#)

Changing Views of Federal Agencies				
	1987/ 1988*	1997/ 1998	2010	97/98-10 Change
% favorable	%	%	%	
Dep't of Education	60	61	40	-21
FDA	74	75	58	-17
Social Security Admin.	--	62	49	-13
EPA	62	69	57	-12
NASA	66	73	61	-12
CDC	--	79	67	-12
Defense Dep't	57	76	67	-9
Postal Service	76	89	83	-6
Justice Dep't	53	56	51	-5
Veterans Admin.**	75	59	57	-2
FBI	78	67	67	0
CIA	52	51	52	+1
IRS	49	38	47	+9
Congress	64	53	26	-27

Pew Research Center March 18-21 Q3c-p.
 * 1987/1988 data from Roper.
 ** From August 1986.

SHARE THIS LINK:

<http://pewrsr.ch/18Zdm43>



Drew DeSilver is a senior writer at Pew Research Center.

[POSTS](#) | [BIO](#) | [TWITTER](#) | [EMAIL](#)

Sign up for our weekly newsletter

Fresh data delivered Saturday mornings



Email address

SIGN UP

RELATED

SHORT READ | MAY 16, 2013

IRS Among Least-Popular Federal Agencies

SHORT READ | OCT 21, 2013

IRS viewed least favorably among federal agencies

SHORT READ | DEC 16, 2015

Americans divided on government's role in space exploration

SHORT READ | OCT 24, 2013

Tea Party Republicans have a love-hate relationship with government

SHORT READ | OCT 3, 2013

Most federal agencies viewed positively, despite frustration and anger with government

MOST POPULAR

SHORT READ | MAR 9, 2022

Majority of workers who quit a job in 2021 cite low pay, no opportunities for advancement, feeling disrespected

FEATURE | NOV 9, 2021

Political Typology Quiz

SHORT READ | JAN 17, 2019

Where Millennials end and Generation Z begins

REPORT | JAN 9, 2020

Trends in income and wealth inequality

SHORT READ | DEC 9, 2021

Gasoline costs more these days, but price spikes have a long history and happen for a host of reasons

Pew Research Center 

1615 L St. NW, Suite 800
Washington, DC 20036
USA
(+1) 202-419-4300 | Main
(+1) 202-857-8562 | Fax
[\(+1\) 202-419-4372 | Media](#)
[Inquiries](#)

RESEARCH TOPICS

Politics & Policy

International Affairs

Immigration & Migration

Race & Ethnicity

Religion

Family & Relationships

Economy & Work

Science

Internet & Technology

News Habits & Media


FOLLOW US

 Email Newsletters

 Facebook

 Twitter

 Tumblr

 YouTube

[Generations & Age](#)

[Methodological Research](#)

 [RSS](#)

[Gender & LGBT](#)

[Full topic list](#)

ABOUT PEW RESEARCH CENTER Pew Research Center is a nonpartisan fact tank that informs the public about the issues, attitudes and trends shaping the world. It conducts public opinion polling, demographic research, media content analysis and other empirical social science research. Pew Research Center does not take policy positions. It is a subsidiary of [The Pew Charitable Trusts](#).

[Copyright 2022 Pew Research Center](#) [About](#) [Terms & Conditions](#) [Privacy Policy](#) [Reprints, Permissions & Use Policy](#)
[Feedback](#) [Careers](#)

PRESS RELEASES (/PRESS-RELEASES)

*For all press release inquiries, please reach out to Theresa Meyer (Theresa.Meyer@mail.house.gov (mailto:Theresa.Meyer@mail.house.gov))

Emmer Leads Bipartisan Blockchain Caucus Letter to the IRS Ahead of Tax Day Urging Virtual Currency Guidance (/press-releases?ID=09CC0055-9DC1-47C5-A8FB-ADC9E615BA04)

April 11, 2019

Washington, DC - Congressman Emmer (MN-06) along with his fellow co-chairs of the Congressional Blockchain Caucus have joined together to send a bipartisan letter to the IRS requesting guidance on how to report virtual currency ahead of tax day. Congressman Emmer was joined by a total of 20 of his colleagues.

In 2014, the IRS issued guidance which treats digital assets like property. Since then, no guidance has been issued on a number of reporting questions. Taxpayers deserve clarity on several basic unanswered questions regarding federal taxation of these emerging exchanges of value.

It has been over a decade since the IRS National Taxpayer Advocate identified, in its 2008 Annual Report, that the ambiguous tax treatment of virtual property and currency transactions was one of "the most serious problems encountered by taxpayers," and nearly five years since the IRS released preliminary guidance on the issue.

While initial guidance was provided, ambiguity around basic questions of how taxpayers should calculate and track the basis of their virtual currency holdings is unacceptable. According to a recent report from Coin Center (https://iqconnect.lmhostediq.com/iqextranet/iqClickTrk.aspx?&cid=MN06TE&crop=14548QQQ7989527QQQ5302658QQQ7229875&report_id=&redirect=https%3a%2f%2fcoincenter.org%2fentry%2fcrypto-tax-questions&redir_log=804324449266353), the 2014 guidance by the IRS failed to address fundamental tax questions, and repeated requests to the IRS for additional clarity have been made by a variety of entities. It also indicates that rather than providing clarity, the IRS has instead increased enforcement activities against taxpayers who "misreport" their cryptocurrency transactions.

"Guidance is long overdue and essential to proper reporting of these emerging assets. The bipartisan support this letter has received should send a clear message to the IRS that clear guidelines for reporting virtual currency are necessary." **Said Emmer**, "My colleagues and I are optimistic that the IRS will issue the guidance needed for taxpayers struggling with these reporting requirements."

Signers include Bill Foster (D-IL), David Schweikert (R-AZ), Darren Soto (D-FL), Patrick McHenry (R-NC), Jim McGovern (D-MA), French Hill (R-AR), Terri Sewell (D-AL), Warren Davidson (R-OH), Stephen Lynch (D-MA), Ted Budd (R-NC), Eric Swalwell (D-CA), Trey Hollingsworth (R-IN), Ed Perlmutter (D-CO), Greg Gianforte (R-MT), Josh Gottheimer (D-NJ), Mark Meadows (R-NC), Lance Gooden (R-TX), Matt Gaetz (R-FL), Ted S. Yoho, D.V.M. (R-FL), and Bryan Steil (R-WI).

Read the full letter here (https://iqconnect.lmhostediq.com/iqextranet/iqClickTrk.aspx?&cid=MN06TE&crop=14548QQQ7989527QQQ5302658QQQ7229875&report_id=&redirect=https%3a%2f%2femmer.house.gov%2fsites%2femmer.house.gov%2ffiles%2f20

https://iqconnect.lmhostediq.com/iqextranet/iqClickTrk.aspx?&cid=MN06TE&crop=14548QQQ7989527QQQ5302658QQQ7229875&report_id=&redirect=https%3a%2f%2femmer.house.gov%2fsites%2femmer.house.gov%2ffiles%2f20

###

Permalink: <https://emmer.house.gov/2019/4/emmer-leads-bipartisan-blockchain-caucus-letter-irs-ahead-tax-day-urging>
(<https://emmer.house.gov/2019/4/emmer-leads-bipartisan-blockchain-caucus-letter-irs-ahead-tax-day-urging>)



Report to the Ranking Member,
Committee on Ways and Means, House
of Representatives

February 2020

VIRTUAL CURRENCIES

Additional Information Reporting and Clarified Guidance Could Improve Tax Compliance

GAO Highlights

Highlights of [GAO-20-188](#), a report to the Ranking Member, Committee on Ways and Means, House of Representatives

Why GAO Did This Study

Virtual currencies, such as bitcoin, have grown in popularity in recent years. Individuals and businesses use virtual currencies as investments and to pay for goods and services. GAO was asked to review IRS's efforts to ensure compliance with tax obligations for virtual currencies.

This report examines (1) what is known about virtual currency tax compliance; (2) what IRS has done to address virtual currency tax compliance risks; (3) the extent to which IRS's virtual currency guidance meets taxpayer needs; and (4) whether additional information reporting on virtual currency income could assist IRS in ensuring compliance.

GAO reviewed IRS forms and guidance and interviewed officials at IRS, FinCEN, and other federal agencies, as well as tax and virtual currency stakeholders.

What GAO Recommends

GAO is recommending that IRS clarify that part of the 2019 guidance is not authoritative and take steps to increase information reporting, and that FinCEN and IRS address how foreign asset reporting laws apply to virtual currency. IRS agreed with the recommendation on information reporting and disagreed with the other two, stating that a disclaimer statement is unnecessary and that it is premature to address virtual currency foreign reporting. GAO believes a disclaimer would increase transparency and that IRS can clarify foreign reporting without waiting for future developments in the industry. FinCEN agreed with GAO's recommendation.

View [GAO-20-188](#). For more information, contact James R. McTigue, Jr., at (202) 512-9110 or mctiguej@gao.gov

February 2020

VIRTUAL CURRENCIES

Additional Information Reporting and Clarified Guidance Could Improve Tax Compliance

What GAO Found

Taxpayers are required to report and pay taxes on income from virtual currency use, but the Internal Revenue Service (IRS) has limited data on tax compliance for virtual currencies. Tax forms, including the information returns filed by third parties such as financial institutions, generally do not require filers to indicate whether the income or transactions they report involved virtual currency.

IRS also has taken some steps to address virtual currency compliance risks, including launching a virtual currency compliance campaign in 2018 and working with other agencies on criminal investigations. In July 2019, IRS began sending out more than 10,000 letters to taxpayers with virtual currency activity informing them about their potential tax obligations.

IRS's virtual currency guidance, issued in 2014 and 2019, addresses some questions taxpayers and practitioners have raised. For example, it states that virtual currency is treated as property for tax purposes and that using virtual currency can produce taxable capital gains. However, part of the 2019 guidance is not authoritative because it was not published in the Internal Revenue Bulletin (IRB). IRS has stated that only guidance published in the IRB is IRS's authoritative interpretation of the law. IRS did not make clear to taxpayers that this part of the guidance is not authoritative and is subject to change.

Examples of Virtual Currency Transactions that Can Produce Taxable Capital Gains



Source: GAO analysis of Internal Revenue Service guidance. | GAO-20-188

Information reporting by third parties, such as financial institutions, on virtual currency is limited, making it difficult for taxpayers to comply and for IRS to address tax compliance risks. Many virtual currency transactions likely go unreported to IRS on information returns, due in part to unclear requirements and reporting thresholds that limit the number of virtual currency users subject to third-party reporting. Taking steps to increase reporting could help IRS provide taxpayers useful information for completing tax returns and give IRS an additional tool to address noncompliance.

Further, IRS and the Financial Crimes Enforcement Network (FinCEN) have not clearly and publicly explained when, if at all, requirements for reporting financial assets held in foreign countries apply to virtual currencies. Clarifying and providing publicly available information about those requirements could improve the data available for tax enforcement and make it less likely that taxpayers will file reports that are not legally required.

Contents

Letter		1
	Background	3
	Data on Tax Compliance for Virtual Currencies Are Limited	10
	IRS Has Taken Some Steps to Address Virtual Currency Compliance Risks and Has Shared Information across Multiple Agencies	13
	IRS's Virtual Currency Guidance Meets Some Taxpayer Needs, but IRS Did Not Address Applicability of Frequently Asked Questions	17
	Third-Party Information Reporting on Virtual Currency Is Limited, and Foreign Account Reporting Requirements Are Unclear	22
	Conclusions	32
	Recommendations for Executive Action	33
	Agency Comments and Our Evaluation	33
Appendix I	Objectives, Scope, and Methodology	36
Appendix II	Comments from the Internal Revenue Service	39
Appendix III	Comments from the Financial Crimes Enforcement Network	42
Appendix IV	GAO Contact and Staff Acknowledgments	43
Figures		
	Figure 1: Example of How a Virtual Currency Operates Using Blockchain, a Distributed Ledger Technology	4
	Figure 2: Examples of Virtual Currency Transactions That Can Affect Taxes	8
	Figure 3: Tax Implications of Paying for Goods Using Virtual Currencies	9
	Figure 4: Effect of Third-Party Information Reporting on Individual Income Tax Compliance, Tax Years 2011-2013	27

Abbreviations

CFTC	Commodity Futures Trading Commission
CI	Criminal Investigation division
FAQs	frequently asked questions
FATCA	Foreign Account Tax Compliance Act
FBAR	Report of Foreign Bank and Financial Accounts
FBI	Federal Bureau of Investigation
FinCEN	Financial Crimes Enforcement Network
IRB	Internal Revenue Bulletin
IRS	Internal Revenue Service
J5	Joint Chiefs of Global Tax Enforcement
LB&I	Large Business and International division
NRP	National Research Program
RAAS	Research, Applied Analytics, and Statistics
SAR	Suspicious Activity Report
SB/SE	Small Business/Self-Employed division
SEC	Securities and Exchange Commission
TIGTA	Treasury Inspector General for Tax Administration
Treasury	Department of the Treasury
VCIT	Virtual Currency Issue Team

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



February 12, 2020

The Honorable Kevin Brady
Ranking Member
Committee on Ways and Means
House of Representatives

Dear Mr. Brady:

Virtual currencies—digital representations of value that generally are not government issued—have grown in popularity since their introduction more than a decade ago. According to the Internal Revenue Service (IRS), there are currently more than 5,000 known virtual currencies. Individuals and businesses use virtual currencies as investments and to make or accept payments for goods and services, among other uses. These virtual currencies account for the equivalent of hundreds of millions of dollars or more in daily transactions. The growth of virtual currencies has raised questions about whether taxpayers who use them are fully meeting their tax obligations.

According to IRS guidance, virtual currencies are treated as property for tax purposes and income from virtual currency use is reportable on tax returns. If taxpayers who use virtual currencies do not comply with their tax obligations, they contribute to the tax gap, the difference between taxes that are owed and actually paid. In September 2019, IRS estimated an average annual gross tax gap of \$441 billion for tax years 2011 to 2013.

You asked us to review IRS's efforts related to virtual currency tax compliance, guidance, and information reporting, which involves third parties, such as financial institutions, reporting information on taxpayer income or transactions to IRS and taxpayers. This report (1) describes what is known about virtual currency tax compliance; (2) describes the steps IRS has taken to address virtual currency tax compliance risks; (3) evaluates the extent to which IRS's virtual currency guidance meets taxpayer needs; and (4) evaluates whether additional information reporting could assist IRS in ensuring compliance.

To describe what is known about virtual currency tax compliance and the steps IRS has taken to address virtual currency tax compliance risks, we reviewed IRS documentation on the agency's virtual currency tax enforcement efforts, including information about the Large Business and

International Division's virtual currency compliance campaign, which was launched in 2018 to address noncompliance related to the use of virtual currency through outreach and examinations. We interviewed IRS officials about any data the agency had on virtual currency tax compliance. For virtual currency tax compliance issues, we also interviewed a nongeneralizable selection of tax practitioners, tax attorneys, virtual currency industry advocates, and virtual currency exchange executives.¹ We selected these stakeholders to interview using a snowball sampling approach, and, in total, we interviewed five individual stakeholders and representatives of 10 entities. We also interviewed officials from the Financial Crimes Enforcement Network (FinCEN), Commodity Futures Trading Commission (CFTC), and Securities and Exchange Commission (SEC) about coordination efforts that have been made across agencies regulating virtual currencies.

To evaluate the extent to which IRS's virtual currency guidance meets taxpayer needs, we reviewed IRS's guidance specific to virtual currency, including Notice 2014-21, issued in March 2014, as well as Revenue Ruling 2019-24 and Frequently Asked Questions (FAQs) released in October 2019. We also reviewed and analyzed all of the public comments IRS had received on Notice 2014-21 as of August 19, 2019. To assess the reliability of these data, we requested information from IRS to identify the quality controls in place to help ensure all comments were processed. We determined that the data were sufficiently reliable for our purposes.

Prior to IRS issuing the Revenue Ruling and FAQs in October 2019, we interviewed the stakeholders mentioned above to determine any taxpayer concerns, any compliance challenges with virtual currency tax obligations, and the extent to which IRS's guidance was meeting taxpayer needs. After the new guidance was issued, we contacted these same stakeholders to gather their perspectives on the new guidance, and received responses from four of the five individuals and six of the 10 organizations we had contacted.

To evaluate whether additional information reporting could assist IRS in ensuring compliance, we reviewed IRS's requirements for information reporting for virtual currency transactions. We interviewed IRS officials about how IRS's third-party and taxpayer information reporting processes

¹Virtual currency exchanges provide a platform where users can transact in different types of virtual currencies or exchange them for government-issued currencies or other virtual currencies.

and forms assist in detecting noncompliance for virtual currencies. We reviewed the websites of a judgmental selection of nine major virtual currency exchanges based in the United States to identify any policies about tax information reporting. We also interviewed the stakeholders mentioned above to obtain their views on what virtual currency information is being reported to IRS; whether additional information reporting would help to ensure tax compliance; and, in interviews with executives from two virtual currency exchanges, what burden, if any, information reporting does or could impose on virtual currency exchanges and virtual currency users.

We conducted this performance audit from October 2018 to February 2020 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Types and Uses of Virtual Currency

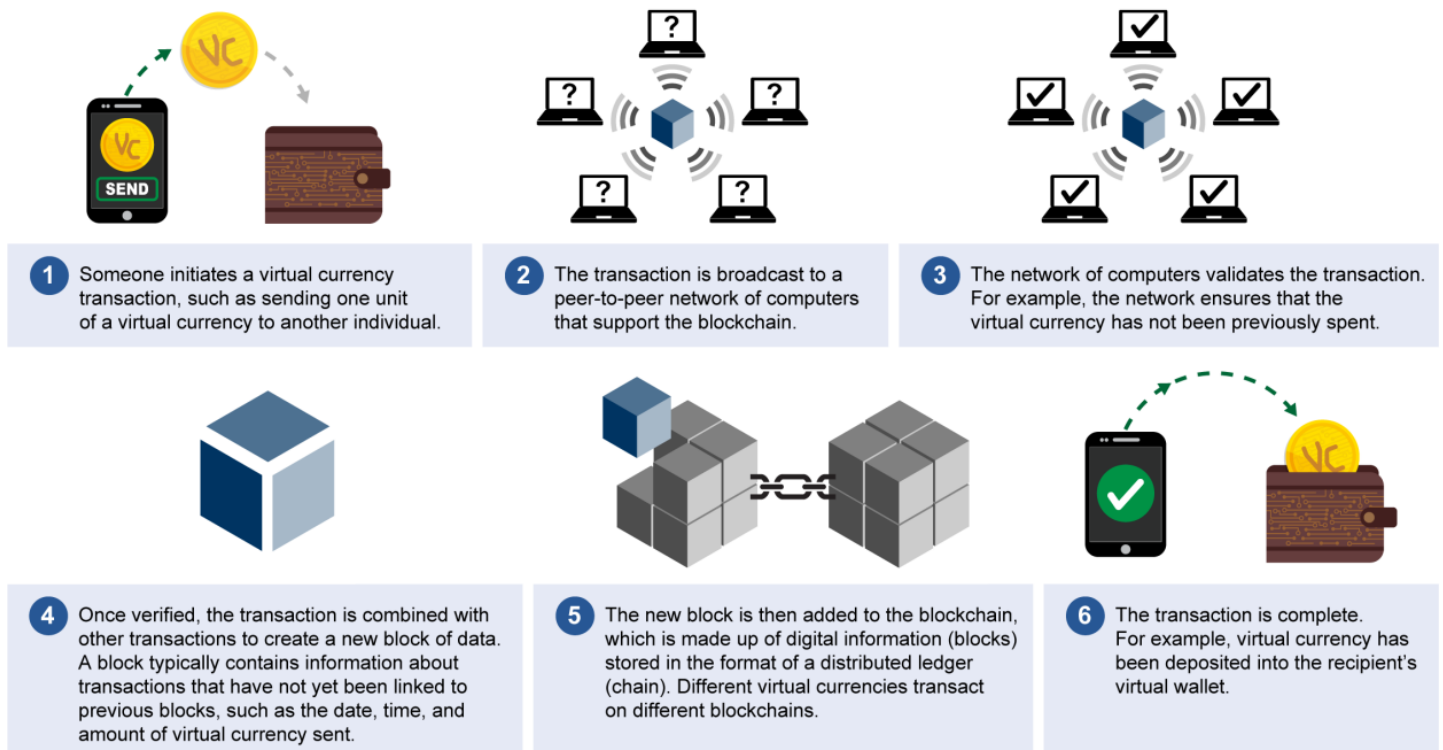
While there is no statutory definition for virtual currency, IRS guidance has described virtual currency as a digital representation of value that functions as a medium of exchange, a unit of account, or a store of value.² Some virtual currencies can be used to buy real goods and services and can be exchanged for U.S. dollars or other currencies.

A cryptocurrency is a type of virtual currency that employs encryption technology and operates on distributed ledger technology, such as blockchain. Distributed ledger technology allows for users across a computer network to verify the validity of transactions potentially without a central authority. For example, a blockchain is made up of digital information (blocks) recorded in a public or private database in the format of a distributed ledger (chain). The ledger permanently records, in a chain of cryptographically secured blocks, the history of transactions that take place among the participants in the network. For the purposes of this

²The term virtual currency is sometimes used interchangeably with other terms, such as digital asset or cryptocurrency. The term digital asset, as used by the Securities and Exchange Commission, refers to an asset that is issued and transferred using distributed ledger technology, including, but not limited to, virtual currencies.

report, we use the term virtual currency as a broad term that includes both cryptocurrencies, which use distributed ledger technology, and digital units of exchange that do not use that technology but still meet IRS's definition of a convertible virtual currency, as defined in Notice 2014-21.³ Figure 1 shows a simplified representation of how distributed ledger technology is used to circulate virtual currencies.

Figure 1: Example of How a Virtual Currency Operates Using Blockchain, a Distributed Ledger Technology



Source: GAO. | GAO-20-188

Note: This figure is a simplified depiction and does not portray how all blocked distributed ledger processes function.

Bitcoin, which emerged in 2009, is the first and most widely circulated blockchain-based cryptocurrency. Bitcoins are created through a process

³For more information, see GAO, *Science and Tech Spotlight: Blockchain & Distributed Ledger Technologies*, [GAO-19-704SP](#) (Washington, D.C.: Sept. 16, 2019).

called mining. Bitcoin miners download software to solve complex equations to verify the validity of transactions taking place on the network, and the first miner to solve a problem is awarded coins in return. Once a problem is solved, the transactions are added as a new block to the distributed ledger.

Users transact in virtual currencies electronically through a network, and may use virtual wallets to manage their virtual currency.⁴ Some virtual currencies can be used as investments and to purchase goods and services in the real economy. For example, some retailers accept virtual currency as a form of payment. Virtual currency exchanges provide a platform where users can transact in different types of virtual currencies or exchange them for government-issued currencies or other virtual currencies.

Estimates of the Size of the Virtual Currency Market

The fair market value of some virtual currencies has changed dramatically over time. For example, according to one index, the average value of one bitcoin was just under \$20,000 in mid-December 2017.⁵ By early February 2018, one bitcoin was valued at about \$7,000, before falling below \$4,000 in December 2018, and again rising to over \$9,000 in November 2019.

The size of the virtual currency market is unknown due to limitations in available data. For example, one recent analysis concluded that a widely cited source for data about bitcoin trading included exaggerated data that gave an inflated impression of the size of the actual market.⁶

⁴Virtual wallets do not store money like traditional wallets, as there is no storage of digital coins following a transaction between users. Virtual wallets can store public keys, private keys, and addresses. Public keys are used to create addresses and verify signatures generated with private keys. Addresses function like account numbers used to send and receive virtual currencies. Private keys are used to sign transactions. For example, when one user sends virtual currency to another user, the sender signs off on the transfer of the virtual currency from the sender's address to the recipient's address. To be able to spend the virtual currency, the recipient must know the private key associated with the recipient's address. The transaction is signified by a transaction record on the blockchain and a change in balance of the users' addresses.

⁵<https://coinmarketcap.com/currencies/bitcoin/historical-data/> (accessed December 4, 2019).

⁶Matthew Hougan, Hong Kim, and Micah Lerner, *Economic and Non-Economic Trading in Bitcoin: Exploring the Real Spot Market for the World's First Digital Commodity* (Bitwise Asset Management, May 2019).

Nonetheless, there are data that may provide some context for the size of this market:⁷

- As of April 2019, 10 major virtual currency exchanges collectively handled an average daily trading volume in bitcoin of more than \$500 million, according to Bitwise. For comparison, the Federal Reserve Banks' Automated Clearing House (a traditional payment processor) processed \$103 billion in payment transactions on average per day in 2018.
- According to one index, the total market capitalization of bitcoin, the most widely circulated virtual currency, is estimated to have ranged between \$60 billion and \$225 billion between December 2018 and October 2019.⁸
- As of November 2019, Coinbase, a large U.S.-based cryptocurrency exchange, reports a user base of more than 30 million.
- According to economists at the Federal Reserve Bank of New York, a 2018 survey they conducted found that 85 percent of respondents had heard of cryptocurrencies, 5 percent currently or previously owned cryptocurrency, and 15 percent reported that they were considering buying cryptocurrency.⁹

Regulation of Virtual Currency

Federal agencies, including CFTC, FinCEN, and SEC, have jurisdiction over various aspects of virtual currency markets and market participants. In May 2014, we reported on the federal financial regulatory and law enforcement agency responsibilities related to the use of virtual currencies and their associated challenges.¹⁰ These challenges include money laundering, transfers of funds across borders, and consumer and investor protection issues. We also reported on the regulatory complexity for virtual currencies and the approaches that federal and state regulators

⁷Given these limitations, we did not test the reliability of data. We provide some figures to provide context for the possible size of the virtual currency market.

⁸<https://blockchain.info> (accessed November 5, 2019).

⁹Sean Hundtofte, Michael Lee, Antoine Martin, and Reed Orchinik, "Deciphering Americans' Views on Cryptocurrencies," Federal Reserve Bank of New York *Liberty Street Economics* (blog), accessed on April 23, 2019, <https://libertystreeteconomics.newyorkfed.org/2019/03/deciphering-americans-views-on-cryptocurrencies.html>.

¹⁰See GAO, *Virtual Currencies: Emerging Regulatory, Law Enforcement, and Consumer Protection Challenges*, [GAO-14-496](#) (Washington, D.C.: May 29, 2014).

have taken to their regulation and oversight.¹¹ For example, CFTC has taken the position that bitcoin and ether, another virtual currency, meet the definition of a commodity provided in the Commodity Exchange Act. SEC has determined that some virtual currencies may be designated as securities, based on the characteristics of how they are offered and sold.¹² FinCEN determined that certain virtual currency businesses would be money transmitters under the Bank Secrecy Act, subject to regulation as money services businesses.¹³

Tax Treatment of Virtual Currency

According to IRS guidance, convertible virtual currencies—which have an equivalent value in real currency or act as a substitute for real currency—are to be treated as property for tax purposes.¹⁴ Among other things, this classification means that income, including gains, from virtual currency transactions is reportable on taxpayers' income tax returns. Therefore, a payment for goods or services made using virtual currency may be subject to tax to the same extent as any other payment made in property. Figure 2 illustrates examples of how virtual currency transactions can affect taxes.

¹¹See GAO, *Financial Technology: Information on Subsectors and Regulatory Oversight*, [GAO-17-361](#) (Washington, D.C.: Apr. 19, 2017).

¹²Securities and Exchange Commission, Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, Exchange Act Rel. No. 81207 (July 25, 2017).

¹³FinCEN, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," FIN-2019-G001, May 9, 2019, <https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf>.

¹⁴IRS Notice 2014-21.

Figure 2: Examples of Virtual Currency Transactions That Can Affect Taxes

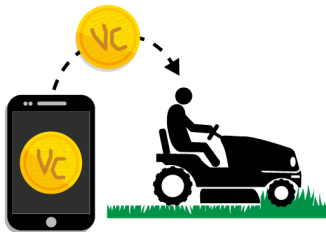
Transactions That Could Affect Taxable Income



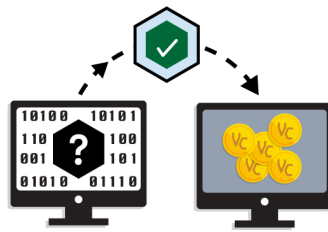
Selling virtual currency for U.S. dollars.



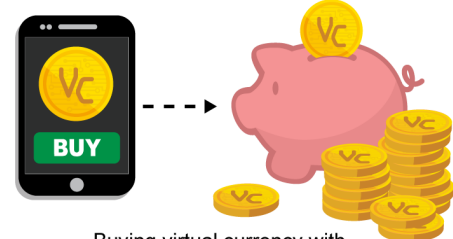
Exchanging one type of virtual currency for another.



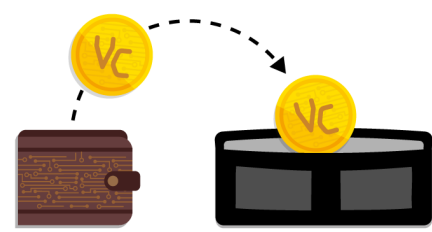
Receiving virtual currency for services.



Mining virtual currency.



Buying virtual currency with dollars and holding on to it.



Sending virtual currency to a different virtual wallet or account with the same owner.

Source: GAO analysis of Internal Revenue Service guidance. | GAO-20-188

Taxpayers using virtual currency must keep track of transaction-level information, such as the fair market value of the virtual currency at the time it was obtained, to determine tax basis and calculate gains or losses. The gain or loss from the sale or exchange of virtual currency is characterized as either a capital gain or loss or an ordinary gain or loss, depending on whether the virtual currency is held as a capital asset.¹⁵

¹⁵According to IRS Notice 2014-21, a taxpayer generally realizes a capital gain or loss on the sale or exchange of virtual currency that is a capital asset in the hands of the taxpayer. For example, stocks, bonds, and other investment property are generally capital assets. A taxpayer generally realizes ordinary gain or loss on the sale or exchange of virtual currency that is not a capital asset in the hands of the taxpayer. Inventory and other property held mainly for sale to customers in a trade or business are examples of property that is not a capital asset. Capital gains may be subject to lower tax rates than ordinary gains. Capital gains and losses are classified as long-term or short-term. Generally, if a taxpayer holds the asset for more than one year before disposing of it, the capital gain or loss is long-term. If a taxpayer holds it one year or less, the capital gain or loss is short-term. For more information, see IRS Publication 544, *Sales and Other Dispositions of Assets*.

Taxpayers are required to report their gains or losses from virtual currency on their tax returns, including Form 1040, *U.S. Individual Income Tax Return*, and Form 8949, *Sales and Other Dispositions of Capital Assets*, for capital gains or losses. Figure 3 shows one example of how using virtual currencies could result in a capital gain or loss.

Figure 3: Tax Implications of Paying for Goods Using Virtual Currencies



Source: GAO analysis of Internal Revenue Service guidance. | GAO-20-188

Data on Tax Compliance for Virtual Currencies Are Limited

Tax and Information Returns Do Not Specifically Capture Information on Virtual Currency Income and Transactions

IRS has limited data on tax compliance for virtual currency use, partly because the forms taxpayers use to report their taxable income do not require them to identify whether the source of their income is from virtual currency use. Likewise, information returns that third parties, such as employers, financial institutions, or other entities, file to report taxpayer income or transactions do not include space for, or direction to, indicate if the income or transactions reported involved a virtual currency.

In 2016, the Treasury Inspector General for Tax Administration (TIGTA) found that IRS had not developed a methodology for gathering data on virtual currency use in taxable transactions that would help to analyze the risk of noncompliance and to estimate its significance. TIGTA recommended that IRS revise third-party information returns to identify the amounts of virtual currency used in taxable transactions. IRS agreed with the recommendation, but stated that it faced other higher priority funding needs, and did not consider modifying information reporting forms to be a priority at the time. As of February 5, 2020, IRS has not implemented any changes to these information returns to include information about virtual currency use.

However, IRS added a question about virtual currency to Schedule 1, *Additional Income and Adjustments to Income*, of Form 1040 for tax year 2019. Individual taxpayers use Schedule 1 to report additional income, such as capital gains, unemployment compensation, prize or award money, and gambling winnings. IRS added a question asking if taxpayers received, sold, sent, exchanged, or otherwise acquired any financial interest in any virtual currency during the tax year. Only taxpayers who are otherwise required to file Schedule 1 or who would answer “yes” to the question need to file this schedule. According to IRS officials responsible for examining tax returns, IRS’s focus is on ensuring taxpayers are reporting all of their taxable income and it is not necessary to distinguish between virtual currency transactions and other property transactions being reported.

IRS Has Data on a Small Number of Taxpayers

Because IRS forms have not required taxpayers to explicitly identify income from virtual currency, IRS uses data from other sources to inform compliance decisions and research. These sources include:

- **Searches of tax return databases.** For tax years 2013 to 2015, IRS searched electronically filed Forms 8949 to identify how often taxpayers included language in the property description to indicate the transaction likely involved bitcoin, the most widely traded virtual currency at the time. For the 3 years, IRS identified fewer than 900 taxpayers who reported virtual currency activity each year. IRS officials said that due to the time and resources required to generate these data, IRS did not generate these filing statistics for tax years 2016 or later. By comparing these data to the size of the bitcoin market, IRS concluded that many taxpayers were likely not reporting income from virtual currency use.
- **Third party information reports.** To address tax noncompliance risks for virtual currencies, in December 2016, IRS served a John Doe summons to Coinbase, a U.S.-based cryptocurrency exchange.¹⁶ After IRS later narrowed the scope of the summons, it requested identifying and transactional data for all Coinbase users with a U.S. address, U.S. telephone number, U.S. email domain, or U.S. bank account that transacted with Coinbase between January 1, 2013, and December 31, 2015 that had the equivalent of \$20,000 in any one transaction type (a buy, sell, send, or receive) in any year during that period. According to an announcement posted on Coinbase's website, on February 23, 2018, Coinbase notified approximately 13,000 customers that it expected to deliver information about their accounts to IRS within 21 days.¹⁷ In addition, IRS officials stated that IRS had received information returns from a small number of virtual currency exchanges for tax year 2017.

¹⁶A John Doe summons is a court-ordered summons that allows IRS to seek information about all taxpayers in a certain group, such as those with accounts at a certain financial institution, without knowing individual identities beforehand. The law authorizing a John Doe summons requires IRS to establish in a federal court proceeding that the summons relates to the investigation of a particular person or ascertainable group or class of persons; there is a reasonable basis to believe that the targeted person or group may fail or may have failed to comply with tax laws; and that the information is not readily available from other sources. 26 U.S.C. § 7609(f).

¹⁷"IRS Notification," Coinbase, accessed October 3, 2019, <https://support.coinbase.com/customer/portal/articles/2924446-irs-notification>. Due to taxpayer privacy protections, we are unable to report on whether IRS received these data or not.

-
- **Third-party reports of potential fraud.** IRS also has access to information on potential fraud reported to IRS and FinCEN by third parties. Financial institutions and money services businesses, which could include virtual currency exchanges, are to file a Suspicious Activity Report (SAR) if they observe or identify suspicious financial activity.¹⁸ SAR reporting can help IRS in identifying potential income underreporting, money laundering, and other potential tax-related violations and crimes.¹⁹ IRS may also receive information about tax noncompliance involving virtual currencies from whistleblowers and other referral programs.
 - **Voluntary disclosures by taxpayers.** In March 2019, IRS updated Form 14457, *Voluntary Disclosure Practice Preclearance Request and Application*, to include a space specifically for taxpayers to disclose that they have unreported virtual currency income. IRS's Criminal Investigation division (CI) reviews the forms IRS receives to ensure they meet criteria of eligibility and timeliness, and that the disclosure does not apply to illegal sources of income. CI sends forms that meet the criteria to two of IRS's civil operating divisions—Large Business & International (LB&I) and Small Business/Self-Employed (SB/SE)—for review.²⁰ According to IRS officials, the addition of virtual currency to the form was made to assist IRS employees in routing the forms to the correct subject matter experts in the civil operating divisions.

IRS Included Virtual Currencies in Research Projects

According to officials with IRS's Research, Applied Analytics, and Statistics (RAAS) division, RAAS had begun some virtual currency research projects to better understand virtual currency tax compliance. One project, which RAAS completed, was to develop compliance profiles for taxpayers that LB&I had identified through its compliance efforts as having virtual currency activity. RAAS officials also said that they are enhancing their use of a range of third-party information reporting, including reporting of virtual currency activity, to improve IRS's ability to

¹⁸31 U.S.C. § 5318(g) provides for the reporting of suspicious activities. FinCEN's regulations require money service businesses to file reports on any suspicious transaction relevant to a possible violation of law or regulation. 31 C.F.R. § 1022.320.

¹⁹Internal Revenue Manual Part 4, Chapter 26, Section 14.

²⁰Criminal and civil matters are handled separately at IRS. IRS's civil divisions, which include LB&I and SB/SE, take administrative actions to enforce the tax code, including assessing tax and imposing civil penalties as appropriate. CI pursues criminal tax offenses that may lead to prosecution, criminal fines, and imprisonment.

assess compliance risks. These efforts focus on use of data from multiple sources to better understand evolving risks and improve estimates of compliance risk. These projects support LB&I, SB/SE, CI, and IRS's broader research, analysis, and statistical reporting needs.

Virtual currency has not been included in past National Research Programs (NRP)—IRS's detailed study of voluntary tax compliance used as the basis for tax gap estimates. The most recent NRP study of individual tax returns was tax years 2011-2013, before virtual currencies became more widely used. RAAS officials said the time frame for the next NRP study of individual tax returns has not yet been determined, but virtual currency may be included in future NRP projects.

IRS Has Taken Some Steps to Address Virtual Currency Compliance Risks and Has Shared Information across Multiple Agencies

IRS Has Trained Staff on Virtual Currency and Begun Civil Enforcement Activities

In December 2013, IRS established the Virtual Currency Issue Team (VCIT) to study virtual currencies and related compliance issues. According to IRS officials, the VCIT aimed to learn about virtual currencies, educate examiners about them, and develop examination techniques to identify and address virtual currency tax compliance risks. In 2015, the VCIT provided two training lessons for examiners on the terminology, technology, and audit issues related to virtual currencies. The VCIT is made up of about 30 individuals and continues to meet periodically to discuss virtual currency issues.

In July 2018, IRS announced the launch of a virtual currency compliance campaign within LB&I to address noncompliance related to individual taxpayers' use of virtual currency through multiple education and enforcement actions, including outreach and examinations. The goals of the compliance campaign include identifying causes of noncompliance using feedback from examination results, using information to identify

additional enforcement approaches to increase compliance and decrease taxpayer burden, and improving examiner knowledge and skills as related to virtual currency transactions. According to IRS officials, the compliance campaign was initiated, in part, to analyze large amounts of data received from third-party sources.

As part of the campaign, IRS developed and delivered several online and in-person training classes on blockchain technology and virtual currencies to its examiners and other staff. The trainings included details on how to identify and understand blockchain transactions and provide examiners with information on how to seek additional information from taxpayers about possible virtual currency use. According to LB&I officials, as examiners provide feedback on what new issues they are seeing in cases involving virtual currency, they will schedule follow-up training sessions to address these new issues.

LB&I has also reached out to a number of external stakeholder groups to gather information and better understand the tax concerns within the virtual currency community. For example, LB&I and the IRS Office of Chief Counsel have spoken to tax practitioner groups, state tax authorities, IRS Nationwide Tax Forum participants, and tax preparation software companies.²¹ According to IRS officials, the discussions they had with tax preparation software companies led to some adding questions to their programs asking taxpayers to enter virtual currency income when preparing their tax returns.

The compliance campaign also aims to assist in developing a comprehensive IRS virtual currency strategy. In addition to leading the compliance campaign, LB&I is also leading a working group focused on cryptocurrency that includes members from across IRS, including LB&I, SB/SE, CI, and the Office of Chief Counsel. This working group reports to the IRS Enforcement Committee, which includes the Deputy Commissioner for Services and Enforcement and the commissioners for each of the operating divisions and CI.

CI has been assisting in analyzing data received from third-party sources to look for potential investigative leads. According to CI officials, CI first reviews the data to identify any taxpayers who are already targets of CI

²¹The Nationwide Tax Forum program is managed by IRS's Office of National Public Liaison. It provides information for tax professionals.

investigations so that LB&I does not use the information in its civil enforcement efforts.²² The officials also said that they were reviewing information from large virtual currency users to identify any ties to criminal activity. However, according to IRS officials, since some of the data IRS has received predate a major uptick in virtual currency activity in 2017, the data that predate these developments are less valuable than more recent data would be, other than to understand the history of an individual's virtual currency usage.

IRS has also begun civil enforcement activities to address virtual currency noncompliance as part of the compliance campaign. In April 2019, LB&I was forwarding cases identified as likely involving virtual currency for examination classification, the process IRS uses to determine which returns to select to examine. Due to the time needed to complete examinations and to allow taxpayers time to exercise their rights, IRS officials said they do not have outcome data from these efforts yet.

In July 2019, IRS began sending out more than 10,000 letters to taxpayers with virtual currency transactions. These letters stated that IRS is aware that the taxpayer may have a virtual currency account. They instructed the taxpayer to ensure that virtual currency income, gains, and losses have been reported appropriately and to file or amend returns as necessary. The letters also provide taxpayers with information on where they can find resources to help them understand their reporting obligations.

IRS Shares Information across Multiple Agencies, Focusing on Criminal Enforcement Efforts That Can Involve Virtual Currencies

According to IRS officials, CI works with a number of federal partners, including FinCEN and the Federal Bureau of Investigation (FBI), among others, in the routine course of its work, which may involve virtual currency issues. According to CI officials, virtual currency does not constitute a new program area that would require a new specific set of policies and procedures. Instead, traditional crimes that CI might investigate may be intertwined with virtual currency use.

²²Internal Revenue Policy Statement 4-26 (formally P-4-84) requires balancing the civil and criminal aspects of investigations to maximize civil enforcement without imperiling criminal prosecution. This policy requires the support of all enforcement divisions/functions to maintain continuing cooperation and coordination. Pursuing both the criminal and the civil aspects of an investigation concurrently may jeopardize the successful completion of the criminal investigation.

CI participates in virtual currency issue information sharing efforts through a number of groups. For example, CI is a monthly participant in the FBI's National Cyber Investigative Joint Task Force, which brings agencies together to share intelligence and work large-scale cases jointly. CI also has agents on site at the National Cyber-Forensics and Training Alliance, a public-private partnership, and at the European Union Agency for Law Enforcement Cooperation. Both entities work on a variety of issues, including virtual currency issues.

CI also participates in some multinational information sharing groups to address virtual currency issues as part of its broader criminal enforcement goals. For example, CI participates in the Joint Chiefs of Global Tax Enforcement (J5), a group of criminal intelligence and tax officials from Australia, Canada, the Netherlands, the United Kingdom, and the United States that launched in mid-2018 to focus on shared cross-national tax risks, including cybercrimes and virtual currency. Among the goals of the J5 are to lead the international community in developing a strategic understanding of offshore tax crimes and cybercrimes, and raise international awareness that the J5 are working together to address international and transnational tax crimes.

Within the Department of the Treasury (Treasury), IRS works with Treasury's Office of Tax Policy when developing any guidance or regulation, including for virtual currency. IRS also works with FinCEN with regard to IRS's delegated authority to administer parts of the Bank Secrecy Act, including *Report of Foreign Bank and Financial Accounts* (FBAR) filings.²³ For example, FinCEN provides training materials to SB/SE examination staff who may come across virtual currency issues in the performance of a Bank Secrecy Act examination. IRS and FinCEN officials also periodically discuss how to apply the Bank Secrecy Act and its implementing regulations to virtual currency transactions.

Given IRS's unique role in administering the federal tax system, it generally does not need to coordinate with other agencies outside of Treasury in developing or issuing virtual currency guidance or taking civil enforcement actions. According to IRS officials, the work of the virtual currency compliance campaign does not involve any other federal agencies.

²³The Bank Secrecy Act and related anti-money laundering authorities and requirements are tools for regulators and law enforcement to detect and deter the use of financial institutions for illicit finance activity.

IRS's Virtual Currency Guidance Meets Some Taxpayer Needs, but IRS Did Not Address Applicability of Frequently Asked Questions

IRS First Issued Virtual Currency Guidance in 2014 and Solicited Public Input to Identify Additional Guidance Needs

IRS first issued virtual currency guidance in 2014, in response to our recommendation.²⁴ In 2013, we found that IRS had not issued guidance specific to virtual currencies and that taxpayers may be unaware that income from transactions using virtual currencies could be taxable. We recommended that IRS provide taxpayers with information on the basic tax reporting requirements for transactions using virtual currencies. In response to this recommendation, IRS issued Notice 2014-21 in March 2014 and published it in the Internal Revenue Bulletin (IRB) in the form of answers to frequently asked questions (FAQs).²⁵

IRS solicited public input on Notice 2014-21 through several means. Within the notice, IRS requested comments from the public regarding other aspects of virtual currency transactions that should be addressed in future guidance by providing a physical and email address to which comments could be submitted. IRS reviewed more than 200 public comments it received to identify topics that were in need of further guidance. Our analysis of the public comments found that the most common topics concerned tax forms and reporting (64 comments), realization of income (45 comments), cost basis (33 comments), and general tax liability (29 comments). Other topics included the tax implications of hard forks and airdrops, mining, and foreign reporting.

²⁴GAO, *Virtual Economies and Currencies: Additional IRS Guidance Could Reduce Tax Compliance Risks*, [GAO-13-516](#) (Washington, D.C.: May 15, 2013).

²⁵The Internal Revenue Bulletin is the authoritative instrument of the Commissioner of Internal Revenue for announcing official rulings and procedures of the Internal Revenue Service and for publishing Treasury Decisions, Executive Orders, Tax Conventions, legislation, court decisions, and other items of general interest.

Virtual currency stakeholders we spoke with, such as tax practitioners, executives at virtual currency exchanges, advocacy groups, and industry representatives also identified these topics as in need of further guidance. Additionally, LB&I officials said they held several sessions to gather information from external stakeholders, such as tax practitioner groups and state tax authorities, to develop a better understanding of what was happening in taxpayer communities.

IRS's 2019 Virtual Currency Guidance Answers Some Taxpayer Concerns, but Presents Additional Challenges for Taxpayers

In October 2019, IRS issued two forms of additional virtual currency guidance, which answered some questions previously raised by the public comments and virtual currency stakeholders. According to IRS, these guidance documents were intended to supplement and expand upon Notice 2014-21.

- Revenue Ruling 2019-24 addresses the tax treatment of hard forks and airdrops following hard forks.²⁶ Specifically, the guidance discusses whether taxpayers have gross income as a result of (1) a hard fork, if they do not receive units of a new virtual currency; or (2) an airdrop of a new virtual currency following a hard fork if they receive units of new virtual currency.
- Additional FAQs provide further examples of how tax principles apply to virtual currency held as a capital asset. Topics addressed include what tax forms to use when reporting ordinary income and capital gains or losses from virtual currency; how to determine fair market value of virtual currencies; when virtual currency use results in taxable income; how to determine cost basis in several scenarios; and when a taxpayer may use the First-In-First-Out accounting method, known as FIFO, to calculate their gains.

However, some virtual currency and tax stakeholders with whom we spoke expressed concern that the 2019 revenue ruling and FAQs leave many questions unanswered and provide confusing responses to others. Their concerns include the following:

²⁶A hard fork occurs when a blockchain splits into two incompatible versions. Such a split may result in the creation of a new type of virtual currency. An airdrop is a distribution of a virtual currency token or coin, usually for free, to virtual currency users, often as a way of promoting new types of virtual currency. For more information on blockchains and forks, see Dylan Yaga, Peter Mell, Nik Roby, and Karen Scarfone, *Blockchain Technology Overview*, National Institute of Standards and Technology Internal Report 8202 (Gaithersburg, MD: October 2018).

-
- **Clarity:** According to some stakeholders, Revenue Ruling 2019-24 is unclear, mostly due to confusion surrounding IRS's usage of technical virtual currency terminology and the situations meant to illustrate IRS's application of the law to hard forks and airdrops. Several tax and virtual currency stakeholders we spoke with said these examples do not accurately explain how virtual currency technology works and therefore may not be helpful to taxpayers looking for guidance on the tax implications of income received as a result of hard forks or airdrops. In public remarks on the new guidance in October 2019, IRS's Chief Counsel stated that terms are not used in a uniform way in the virtual currency industry, but IRS is interested in receiving comments on how virtual currency technology should be described.
 - **Additional topics in need of guidance:** The revenue ruling and additional FAQs do not address several topics raised in the public comments and by stakeholders. For example, the guidance does not clarify foreign asset reporting requirements for virtual currency. The statutory provisions commonly known as the Foreign Account Tax Compliance Act (FATCA) require taxpayers and foreign financial institutions to report on certain financial assets held outside the United States.²⁷ Regulations implementing the Bank Secrecy Act separately require taxpayers to report certain foreign financial accounts to FinCEN on the FBAR form.²⁸ Some practitioners told us that it is unclear whether these requirements apply to virtual currency wallets and exchanges, as we discuss later in this report. Other topics not addressed in the 2019 guidance include mining, like-kind exchanges, and retirement accounts.

²⁷Subtitle A of Title V of the Hiring Incentives to Restore Employment Act is commonly referred to as FATCA. Pub. L. No. 111-147, §§ 501-541, 124 Stat. 71, 97-117 (2010).

²⁸In prior work we found that reporting requirements for foreign financial assets under FATCA overlap with the FBAR reporting requirements. These overlapping requirements—implemented under two different statutes—have resulted in most taxpayers filing Forms 8938, *Statement of Specified Foreign Financial Assets*, also filing FBARs with FinCEN. We recommended that Congress consider amending the Internal Revenue Code, Bank Secrecy Act of 1970, and other statutes, as needed, to address overlap in foreign financial asset reporting requirements for the purposes of tax compliance and detection, and prevention of financial crimes, such as by aligning the types of assets to be reported and asset reporting thresholds, and ensuring appropriate access to the reported information. For more information, see GAO, *Foreign Asset Reporting: Actions Needed to Enhance Compliance Efforts, Eliminate Overlapping Requirements, and Mitigate Burdens on U.S. Persons Abroad*, [GAO-19-180](#) (Washington, D.C.: Apr. 1, 2019).

According to an official from the IRS Office of Chief Counsel, IRS's focus when developing the 2019 guidance was to assist individual taxpayers. Therefore, the topics addressed by the revenue ruling and FAQs were limited to the most common issues that would be applicable to most individual taxpayers. The official told us that if IRS were to develop additional virtual currency guidance in the future, it may focus on a different audience, such as taxpayers involved in virtual currency businesses or exchanges that could be subject to third-party information reporting. Another official stated that issuing guidance on certain topics, including like-kind exchanges, would have taken additional time, and these topics were therefore left unaddressed.

IRS Did Not Include That the 2019 FAQs Are Not Legally Binding

IRS issues thousands of publications in a variety of different forms to help taxpayers and their advisors understand the law; however, IRS has stated that only guidance published in the IRB contains IRS's authoritative interpretation of the law.²⁹ Unlike with the virtual currency FAQs IRS issued in 2014 in the form of a notice, the 2019 FAQs were not published in the IRB. Therefore, the 2019 FAQs are not binding on IRS, are subject to change, and cannot be relied upon by taxpayers as authoritative or as precedent for their individual facts and circumstances. For FAQs not published in the IRB, tax practitioners have noted that sometimes IRS has included a disclaimer noting that the FAQs do not constitute legal authority and may not be relied upon.³⁰ The new virtual currency FAQs do not include such a disclaimer.

²⁹Guidance published in the IRB goes through a multistep clearance process at both Treasury and IRS, involving review and approval by officials in a wide variety of Treasury and IRS offices. The weekly IRB is described as the "authoritative instrument" for publishing official IRS rulings and procedures and tax regulations. The five types of guidance published in the IRB are: regulations, revenue rulings, revenue procedures, notices, and announcements. Tax regulations are also published in the *Federal Register* and codified in the Code of Federal Regulations like other federal agency regulations. Other IRS publications and information are described in the Internal Revenue Manual as "a good source of general information." The form that information in this category can take varies widely, and includes IRS videos, online tools, forms and publications, and FAQs. For more information, see GAO, *Regulatory Guidance Processes: Treasury and OMB Need to Reevaluate Long-standing Exemptions of Tax Regulations and Guidance* GAO-16-720, (Washington, D.C.: Sept. 6, 2016).

³⁰See, for example, IRS, "U.S. Withholding Agent Frequently Asked Questions," updated October 22, 2019, <https://www.irs.gov/businesses/international-businesses/us-withholding-agent-frequently-asked-question>, accessed December 16, 2019.

According to IRS officials, they did not include a disclaimer along with the new FAQs because the FAQs do not contain any substantial new interpretation of the law. IRS officials did not feel that a disclaimer about the limitations of the FAQs was necessary or that it would be helpful to taxpayers. However, the FAQs provide new information, such as a definition of the term “cryptocurrency” and an explanation of how taxpayers can track cost basis for virtual currency.

As we have previously reported, clarity about the authoritativeness of certain IRS publications could be improved by noting any limitations, especially when FAQs provide information to help taxpayers comply with tax law.³¹ Additional explanatory language would help taxpayers understand what type of IRS information is considered authoritative and reliable as precedent for a taxpayer’s individual facts and circumstances.

The first article in IRS’s Taxpayer Bill of Rights—“The Right to Be Informed”—states that taxpayers have the right to know what they need to do to comply with tax laws. The article further states that taxpayers are entitled to clear explanations of the laws and IRS procedures in all forms, instructions, publications, notices, and correspondence. As we have previously reported, just as taxpayers have the right to clear explanations in IRS instructions and publications, taxpayers should be alerted to any limitations that could make some IRS information less authoritative than others.³²

Failing to note any limitations associated with particular guidance could lead to misinterpretation of nonauthoritative information from IRS. If taxpayers make decisions based on guidance that is nonauthoritative, including FAQs, those taxpayers’ confidence in IRS and the tax system could be undermined if the content is later updated and IRS challenges taxpayers’ positions. As we have noted in prior reports, taxpayers’ perception that IRS is fairly and uniformly administering the tax system

³¹[GAO-16-720](#).

³²[GAO-16-720](#).

helps further overall voluntary compliance and lowers IRS's administrative costs.³³

Third-Party Information Reporting on Virtual Currency Is Limited, and Foreign Account Reporting Requirements Are Unclear

Limited Third-Party Information Reporting Makes It Difficult for IRS to Address Compliance Risks

IRS does not receive information returns on some potentially taxable transactions involving virtual currency, which limits its ability to detect noncompliance. Some virtual currency exchanges send information returns to IRS and to customers that provide information about customers' trading activity, but others do not.

Financial institutions and other third parties are to report interest payments, property sales, and other transactions to both taxpayers and IRS using forms known as information returns.

- **Form 1099-K, *Payment Card and Third Party Network Transactions*.** Third parties that contract with a substantial number of unrelated merchants to settle payments between the merchants and their customers are required to issue a Form 1099-K for each merchant that meets the threshold of having more than 200 transactions totaling more than \$20,000 in a year.³⁴
- **Form 1099-B, *Proceeds from Broker and Barter Exchange Transactions*.** Brokers use Form 1099-B to report transactions such

³³See, for example, GAO, *IRS Return Selection: Wage and Investment Division Should Define Audit Objectives and Refine Other Internal Controls*, [GAO-16-102](#) (Washington, D.C.: Dec. 17, 2015); and *IRS Return Selection: Certain Internal Controls for Audits in the Small Business and Self-Employed Division Should Be Strengthened*, [GAO-16-103](#) (Washington, D.C.: Dec. 16, 2015).

³⁴26 U.S.C. § 6050W; 26 C.F.R. §§ 1.6050W-1, 1.6050W-2.

as sales or redemptions of securities, regulated futures contracts, and commodities.³⁵ For certain types of property, brokers must also report cost basis information on Form 1099-B if the information is required.

- **Form 1099-MISC, *Miscellaneous Income*.** Certain payments made in the course of a trade or business—including rents, prizes, and various other types of income—must be reported by the payer on Form 1099-MISC. For most types of income subject to reporting on Form 1099-MISC, payers must file the form only if they made payments totaling at least \$600.³⁶

According to our review of websites for nine major U.S.-based virtual currency exchanges, as of November 2019, two exchanges have policies posted online stating that they report information for some of their customers' virtual currency transactions to IRS on Form 1099-K. One exchange states that it reports customers' transactions on Form 1099-B, a more detailed information return that provides a breakdown of individual virtual currency transactions. Another exchange's website states that it provides Forms 1099, but does not identify the form more specifically. Three exchanges' websites have policies stating that the exchanges do not report customers' transactions on tax forms. The remaining two exchanges do not state on their websites whether or not they file information returns or provide customers with tax forms.

When transactions handled by third parties, such as virtual currency exchanges, go unreported on information returns, it is difficult for IRS to identify and address compliance risks. According to IRS officials and tax practitioners we interviewed, it is difficult for IRS to find out when taxable transactions involving virtual currency are occurring. As discussed earlier in this report, IRS's virtual currency compliance campaign has identified more than 10,000 taxpayers who may not have properly reported virtual currency transactions on tax returns. However, the campaign likely has not identified all taxpayers with underreported virtual currency income. In addition, according to IRS officials, examining tax returns is more

³⁵26 U.S.C. § 6045; 26 C.F.R. § 1.6045-1.

³⁶26 U.S.C. § 6041; 26 C.F.R. §§ 1.6041-1 to 1.6041-10.

resource intensive than the automated processes IRS uses to match tax returns against information returns.³⁷

For taxpayers, limited information reporting by third parties can make it difficult to complete tax returns. Tax practitioners told us that recordkeeping is a challenge for taxpayers who buy and sell virtual currencies. To report virtual currency income accurately under IRS guidance, taxpayers need to report information about each transaction, including cost basis and fair market value at the time virtual currency is disposed of, such as by selling it for cash or another virtual currency on an exchange.

Some taxpayers may not keep their own records of virtual currency transactions, and as a result may lack easy access to the information that would be provided in third-party information returns. When taxpayers do keep these records, they may not know how to report virtual currency transactions on tax forms. As discussed earlier in this report, 64 of the public comments IRS received on Notice 2014-21 were about forms and reporting. For example, some of these 64 comments expressed uncertainty about how to calculate the fair market value of virtual currency at the time of sale; others requested assistance in determining which tax forms to use to report income from virtual currency transactions.

Some virtual currency transactions are not subject to third-party reporting requirements. For example, unless owned by a U.S. payor (including a controlled foreign corporation), virtual currency exchanges operating outside the United States are not required to file information returns such as Forms 1099-K or 1099-B unless the customer or transaction has certain connections to the United States. Some transactions, such as transferring virtual currency directly to a merchant in exchange for goods, generally create no obligation to file any information returns.

Other virtual currency transactions, such as sales of virtual currency for cash through virtual currency exchanges, may be subject to third-party reporting requirements. However, those requirements are not entirely

³⁷The automated underreporter program, through which IRS matches amounts reported on tax returns with amounts reported on information returns submitted by third parties, is one such process. This computer matching program allows IRS to identify discrepancies between tax returns and information returns, and propose automatic changes to taxpayers. Sometimes, if the discrepancy exceeds a certain tax threshold, an automated underreporter reviewer will contact a taxpayer asking for an explanation of the discrepancy or payment if additional taxes are assessed.

clear, and people have interpreted them differently. Tax practitioners we spoke with generally stated that it is not clear whether current regulations require virtual currency exchanges to report customers' trading activity on Forms 1099-K or 1099-B. According to IRS officials, virtual currency exchanges may be subject to the 1099-K reporting requirement if they fall into the legal category of "third party settlement organizations."³⁸ Exchanges are subject to the 1099-B requirement only if they are brokers or barter exchanges. IRS does not have an official position on whether virtual currency exchanges are required to report customers' trading activity on Form 1099-B. There may also be ambiguity regarding when, if at all, reporting on virtual currency sales is required on Form 1099-MISC.

Furthermore, even if exchanges are subject to the 1099-K, 1099-B, or 1099-MISC reporting requirements, these requirements do not cover all taxable transactions. Third-party settlement organizations are required to file Form 1099-K only for customers who make more than 200 transactions in a year that total more than \$20,000. Taxable transactions below that threshold may not be reported. Separately, some transactions carried out by brokers do not need to be reported on Form 1099-B unless they involve cash. For example, taxpayers must report trades between different virtual currencies on tax returns, but brokers may not be required to report such trades on Form 1099-B.³⁹ According to IRS, a virtual currency exchange would be required to file Form 1099-MISC if it has sufficient information, such as the recipient's basis in the virtual currency, to determine whether a payment made to a recipient in exchange for virtual currency gives rise to income for that recipient.

In addition, Forms 1099-K, 1099-B, and 1099-MISC do not always contain all the information that taxpayers need to file accurate tax returns or that IRS needs to monitor compliance. Form 1099-K provides information on the number and gross amount of payments made to the recipient, but does not provide information about individual transactions.⁴⁰

³⁸The term third party settlement organization refers to the central organization that has the contractual obligation to make payment to participating payees of third party network transactions. 26 U.S.C. § 6050W(b)(3), (e).

³⁹26 C.F.R. § 1.6045-1(a)(9) (defining "sale" in terms of a disposition for cash). However, barter exchanges may be required to report trades between different virtual currencies that do not involve cash. 26 C.F.R. § 1.6045-1(f). IRS has not taken an official position on how the rules for barter exchanges apply to virtual currency exchanges.

⁴⁰The content of Form 1099-K follows the requirements set out in the Internal Revenue Code for information reporting by payment settlement entities. 26 U.S.C. § 6050W.

Some tax practitioners we interviewed stated that taxpayers who receive Form 1099-K for virtual currency transactions may find the form unhelpful or confusing. Because the form does not identify specific transactions, it may be difficult to match the aggregate amounts reported on the form with taxpayers' own records of virtual currency transactions. Form 1099-B does provide information about individual transactions, but does not always include or require cost basis information. According to IRS, a Form 1099-MISC that reports a payee's gain does not provide information about that payee's gross proceeds and basis.

Some stakeholders we interviewed mentioned challenges that could make it difficult to implement information reporting at the individual transaction level. For example, it could be difficult to distinguish between taxable dispositions of virtual currency—such as the sale of virtual currency for U.S. dollars—and nontaxable events such as the transfer of virtual currency from a taxpayer's account on an exchange to a personal wallet controlled directly by the same taxpayer. These stakeholders also told us that if exchanges were required to report cost basis information, additional challenges could include tracking the cost basis of virtual currency transferred between exchanges. However, as we have previously reported, cost basis reporting can be particularly valuable for tax compliance.⁴¹ IRS officials told us that they are studying the issue of third-party information reporting, and it is included in IRS's priority guidance plan as of October 2019.⁴²

We have reported that, in general, the extent to which taxpayers accurately report their income is closely aligned with the amount of income that third parties report to them and to IRS.⁴³ For example, according to IRS data for tax years 2011-2013, taxpayers misreported more than half of their income for types of income subject to little or no third-party information reporting (see figure 4). Taxpayers misreported a

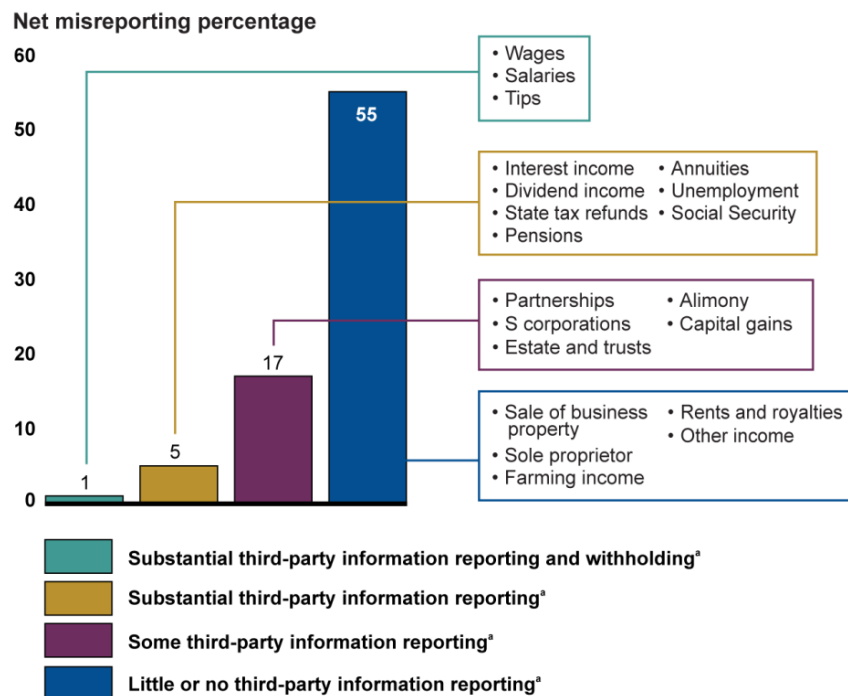
⁴¹GAO, *Tax Gap: Sources of Noncompliance and Strategies to Reduce It*, [GAO-12-651T](#) (Washington, D.C.: Apr. 19, 2012).

⁴²Previously, IRS officials told us that clarifying existing information reporting requirements or adding new requirements specific to virtual currency may require statutory changes to the Internal Revenue Code.

⁴³GAO, *Tax Gap: Multiple Strategies Are Needed to Reduce Noncompliance*, [GAO-19-558T](#) (Washington, D.C.: May 9, 2019); IRS, *Federal Tax Compliance Research: Tax Gap Estimates for Tax Years 2011–2013*, Publication 1415 (Washington, D.C.: September 2019), available at <https://www.irs.gov/pub/irs-pdf/p1415.pdf>.

much lower percentage of their income for types of income subject to at least some information reporting.

Figure 4: Effect of Third-Party Information Reporting on Individual Income Tax Compliance, Tax Years 2011-2013



Source: GAO analysis of Internal Revenue Service (IRS) information. | GAO-20-188

Note: Net misreporting percentage is the net misreported amount divided by the absolute values of the amounts that should have been reported, expressed as a percentage.

^aIRS receives information from third parties that it uses to verify income or deduction amounts that taxpayers report on their tax returns. IRS categorized various line items on the individual income tax return into four different groupings of third-party reporting in IRS Publication 1415, *Federal Tax Compliance Research: Tax Gap Estimates for Tax Years 2011–2013* (Washington, D.C.: September 2019). However, IRS did not provide a scale to define the differences between substantial, some, and little or no third-party information reporting.

Information returns that include details about individual transactions can assist taxpayers by providing information about how to report virtual currency income correctly. For example, in addition to providing transaction details, Form 1099-B instructs recipients where to report transactions on Form 8949 or Schedule D, which are forms used to report capital gains. By contrast, Form 1099-K does not include similar instructions.

One of IRS's strategic goals is to protect the integrity of the tax system by encouraging compliance through administering and enforcing the tax code.⁴⁴ This goal includes identifying and planning for compliance risks proactively, including risks associated with the increasing complexity of the tax base. Further, internal control standards state that management should use quality information to achieve the entity's objectives.⁴⁵ Using quality information requires identifying information requirements and obtaining relevant data from reliable sources.

As discussed above, IRS does not have quality information on many potentially taxable transactions involving virtual currency, in part because information reporting requirements for virtual currency exchanges are unclear, and in part because some information reporting does not include detailed information about specific transactions. As a result, some taxpayers may not be reporting virtual currency transactions properly on their tax returns or paying the full amount of tax owed on those transactions, contributing to the tax gap.

IRS and FinCEN Have Not Clarified Whether Foreign Account Reporting Requirements Apply to Virtual Currency

As previously discussed, two overlapping reporting requirements apply to taxpayers who have foreign financial assets. These two requirements are the *Report of Foreign Bank and Financial Accounts* (FBAR) filings required under the Bank Secrecy Act and the separate reports required by the statutory provisions commonly known as the Foreign Account Tax Compliance Act (FATCA). The federal agencies that administer these requirements have not clarified how taxpayers who hold virtual currency should interpret them.

FATCA Requirements

Under FATCA, taxpayers have an obligation to report certain foreign financial accounts and other assets on IRS Form 8938, *Statement of Specified Foreign Financial Assets*, if the value of those assets exceeds a certain amount. FATCA was enacted in 2010 to reduce offshore tax evasion, and it also requires foreign financial institutions to report detailed information to IRS about their U.S. customers.

Tax practitioners we interviewed told us that there is no generally accepted view about whether FATCA filing requirements apply to virtual

⁴⁴IRS, *Strategic Plan: FY2018—2022*, Publication 3744 (April 2018).

⁴⁵GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: September 2014), 59.

currency holdings, and IRS has not publicly stated a position on how, if at all, FATCA requirements apply to virtual currency holdings for either taxpayers or institutions. Some practitioners stated that in the absence of guidance or information from IRS specifically addressing virtual currency and FATCA, some of their clients report foreign virtual currency accounts because the potential penalties for failing to report, if deemed to be required, are high.⁴⁶ Additionally, several public comments on IRS Notice 2014-21 requested clarification from IRS about whether virtual currency holdings must be reported under FATCA.

The FATCA filing requirements can be difficult for individual taxpayers to interpret, in part because FATCA was enacted before the use of virtual currency became more widespread, and it was not designed to cover nontraditional assets such as virtual currencies. For example, under FATCA, taxpayers must report accounts at foreign financial institutions. A taxpayer who holds virtual currency with an exchange based outside the United States may not know whether the exchange counts as a foreign financial institution under FATCA because this determination involves applying legal criteria to specific facts about how the exchange operates.⁴⁷

Taxpayers must also report foreign nonaccount assets held for investment (as opposed to held for use in a trade or business), such as foreign stock and securities, foreign financial instruments, contracts with non-U.S. persons, and interests in foreign entities.⁴⁸ IRS officials told us that in some situations, virtual currencies could be foreign nonaccount assets, depending on specific facts about how an individual taxpayer holds the virtual currency. However, a taxpayer holding virtual currency may not know whether the virtual currency is considered a specified foreign financial asset because this determination involves applying legal

⁴⁶Nonfiling penalties for individuals can be up to \$10,000 for failure to disclose and an additional \$10,000 for each 30 days of nonfiling after IRS notice of a failure to disclose, for a potential maximum penalty of \$50,000. 26 U.S.C. § 6038D(d); 26 C.F.R. § 1.6038D-8.

⁴⁷A foreign financial institution is defined as a foreign entity that either (1) accepts deposits in the ordinary course of a banking or similar business; (2) as a substantial portion of its business, holds financial assets for the account of others; or (3) is engaged (or holds itself out as being engaged) primarily in the business of investing, reinvesting, or trading in securities, partnership interests, commodities, or any interest (including a futures or forward contract or option) in such securities, partnership interests, or commodities. 26 U.S.C. § 6038D(b)(1); 26 U.S.C. § 1471(d)(4),(5).

⁴⁸26 U.S.C. § 6038D(b)(2).

criteria to specific facts such as whether the virtual currency has a foreign issuer, which the taxpayer may not have sufficient information to determine.

According to IRS officials, they have not issued guidance about virtual currency and FATCA because the instructions for Form 8938 clearly explain how taxpayers are to interpret FATCA requirements. However, those instructions do not mention virtual currency and do not provide information needed to determine whether virtual currency holdings must be reported. For example, the instructions state that a financial account is any depository or custodial account maintained by a foreign financial institution, but do not explain under what circumstances, if any, an account that holds virtual currency could be considered a depository or custodial account.⁴⁹

IRS's Taxpayer Bill of Rights states that taxpayers are entitled to clear explanations of the laws and IRS procedures in all tax forms, instructions, publications, notices, and correspondence. Furthermore, one of IRS's strategic goals is to empower taxpayers by making it easier for them to understand and meet their filing, reporting, and payment obligations.⁵⁰

Without information about how to interpret and apply FATCA requirements to situations involving virtual currency, taxpayers will not know whether they are required to report virtual currency held outside the United States. As a result, they may be underreporting, depriving IRS of data needed to address offshore tax evasion, or overreporting by filing forms that are not required. As we have previously reported, such overreporting creates unnecessary burdens, including financial costs, for taxpayers.⁵¹

⁴⁹The instructions refer to the Treasury regulations for the definitions of the terms "depository account" and "custodial account." For example, a custodial account is defined as "an arrangement for holding a financial instrument, contract, or investment (including, but not limited to, a share of stock in a corporation, a note, bond, debenture, or other evidence of indebtedness, a currency or commodity transaction, a credit default swap, a swap based upon a nonfinancial index, a notional principal contract as defined in § 1.446-3(c), an insurance or annuity contract, and any option or other derivative instrument) for the benefit of another person." This section of the regulations does not define the terms "financial instrument" or "investment." 26 C.F.R. § 1.1471-5.

⁵⁰IRS, *Strategic Plan: FY2018—2022*, Publication 3744 (April 2018).

⁵¹[GAO-19-180](#).

FBAR Requirement

Separate from the requirement to file Form 8938 under FATCA, regulations implementing the Bank Secrecy Act require reporting of financial accounts maintained with financial institutions located outside the United States on the FBAR form.⁵² FinCEN's FBAR regulations predate the widespread use of virtual currency and do not specifically mention virtual currency. Consequently, tax practitioners have raised questions about whether taxpayers are required to include virtual currency holdings in FBAR filings.

In correspondence and interviews, FinCEN officials have stated that, based on their understanding of the regulations, virtual currency does not need to be reported on the FBAR. For example, FinCEN officials told us that FinCEN provides a standard response when members of the public ask FinCEN's Resource Center about reporting virtual currency on the FBAR. The response states, in part, "as of right now, reporting [virtual currency exchange accounts] on the FBAR is not required." Likewise, in March 2019, FinCEN responded in writing to a question from the American Institute of Certified Public Accountants by stating that the FBAR regulations do not define virtual currency held in an offshore account as a type of reportable account.

While FinCEN has provided responses to direct questions, it has not made information about whether foreign virtual currency accounts are subject to the FBAR requirement readily available, such as by posting this information on its website. FinCEN officials stated that FinCEN and IRS had issued a statement on IRS's website in 2014 informing the public that virtual currencies did not need to be reported on the FBAR.⁵³ However, the officials noted that the statement was no longer available on the website, but they did not say when it may have been removed or why. Neither IRS's FBAR Reference Guide nor FinCEN's instructions for filing the FBAR mention virtual currencies.

Internal control standards state that management should externally communicate the necessary quality information to achieve the entity's objectives.⁵⁴ As part of this standard, management should communicate

⁵²31 C.F.R. § 1010.350.

⁵³Under a Memorandum of Agreement signed in 2003, IRS and FinCEN each have responsibilities for certain aspects of the FBAR requirement, and the two agencies work together to interpret and enforce the requirement.

⁵⁴[GAO-14-704G](#), 62.

information that allows external parties, including the general public, to assist the entity in achieving its objectives.

In the absence of a readily available official statement from FinCEN that virtual currencies are not reportable on the FBAR, users of virtual currency may be filing reports that are not legally required. According to some tax practitioners we interviewed, some individuals may report foreign virtual currency accounts on the FBAR even if they believe it is unlikely that they are required to report, because of the high penalties for failing to file required FBARs.⁵⁵ Such filings can create financial costs and unnecessary recordkeeping and other burdens for these individuals.

Conclusions

Virtual currencies can present challenges for enforcement of tax laws, both because they can be circulated without a central authority and because complying with current tax requirements can be confusing and burdensome. IRS has taken important steps to address these challenges, including issuing multiple sets of guidance to clarify how virtual currencies would be treated for tax purposes and carrying out a range of enforcement activities to address noncompliance.

Although IRS's 2019 virtual currency guidance addressed some issues left unresolved by its 2014 guidance, it did not address others, and it has also prompted new concerns among virtual currency stakeholders. Additionally, including information that the 2019 FAQs are not legally binding would enhance taxpayer understanding and could ultimately help enhance taxpayers' confidence in IRS and the tax system.

Currently, much trading activity in virtual currency goes unreported on information returns. In part, this lack of reporting may be because third parties are unclear about whether they are required to report. Limitations in what information returns report related to virtual currencies also constrain the utility of reported information. In general, information reporting is associated with high levels of compliance.

⁵⁵Penalties for failing to file a required FBAR can be up to \$10,000 per violation, if nonwillful, and the greater of \$100,000 or 50 percent of account balances, if willful, for civil penalty assessment prior to August 2, 2016. For penalties assessed after August 1, 2016, whose associated violations occurred after November 2, 2015, the maximum penalties for negligent, nonwillful, and willful violations are adjusted for inflation. 31 C.F.R. § 1010.821. Criminal penalties may also apply for certain willful violations of either FATCA or FBAR requirements.

Additionally, the rules for foreign asset reporting—specifically, the FBARs required by the Bank Secrecy Act and the separate reports required by FATCA—do not clearly address virtual currency, and tax professionals have raised questions about the applicability of these requirements to virtual currency. Clarifying the FATCA requirements and making a statement about the FBAR requirements readily available to the public would help reduce uncertainty about these rules and may result in reduced burden for some taxpayers who may be filing reports that are not required.

Recommendations for Executive Action

We are making a total of four recommendations, including three to IRS and one to FinCEN. Specifically,

The Commissioner of Internal Revenue should update the FAQs issued in 2019 to include a statement that the FAQs may serve as a source of general information but cannot be relied upon by taxpayers as authoritative since they are not binding on IRS. (Recommendation 1)

The Commissioner of Internal Revenue should take steps to increase third-party reporting on taxable transactions involving virtual currency, which could include clarifying IRS's interpretation of existing third-party reporting requirements under the Internal Revenue Code and Treasury Regulations, or pursuing statutory or regulatory changes. (Recommendation 2)

The Commissioner of Internal Revenue should clarify the application of reporting requirements under FATCA to virtual currency. (Recommendation 3)

The Director of FinCEN, in coordination with IRS as appropriate, should make a statement about the application of foreign account reporting requirements under the Bank Secrecy Act to virtual currency readily available to the public. (Recommendation 4)

Agency Comments and Our Evaluation

We provided a draft of this report to IRS, FinCEN, Treasury, SEC, and CFTC for review and comment. In its written comments, which are summarized below and reproduced in appendix II, IRS agreed with one and disagreed with two of the recommendations directed to it. In its written comments, which are summarized below and reproduced in appendix III, FinCEN agreed with the recommendation directed to it. IRS,

Treasury, SEC, and CFTC provided technical comments, which we incorporated as appropriate.

IRS agreed with the recommendation to take steps to increase third-party reporting on taxable transactions involving virtual currency (recommendation 2). IRS stated that it is working with Treasury to develop guidance on third-party reporting under section 6045 of the Internal Revenue Code for certain taxable transactions involving virtual currency. Such guidance, if it aims to increase third-party reporting, would address the intent of the recommendation.

IRS disagreed with the recommendation to add a statement to the 2019 FAQs on virtual currency informing taxpayers that the FAQs provide general information but are not binding on IRS (recommendation 1). IRS stated that the FAQs are illustrative of how longstanding tax principles apply to property transactions. IRS also stated that IRS does not take positions contrary to public FAQs. We continue to believe that including such a statement would provide more transparency and help taxpayers understand the nature of the information provided in the FAQs.

As we state earlier in this report, IRS has included disclaimer statements in other informal FAQs posted on its website. IRS could include a similar statement in the virtual currency FAQs at minimal cost. Alternatively, if IRS intends to be bound by the positions it takes in the current version of the virtual currency FAQs, as the response to this recommendation suggests, it could publish the FAQs in the Internal Revenue Bulletin. Doing so would render a disclaimer statement unnecessary and would satisfy the intent of the recommendation.

IRS disagreed with the recommendation to clarify the application of FATCA reporting requirements to virtual currency (recommendation 3). IRS stated that U.S. exchanges and other U.S. businesses play a significant role in virtual currency transactions carried out by U.S. taxpayers, and therefore it is appropriate for IRS to focus on developing guidance for third-party reporting under section 6045, as discussed above. IRS also stated that guidance on FATCA may be appropriate in the future when the workings of foreign virtual currency exchanges become more transparent.

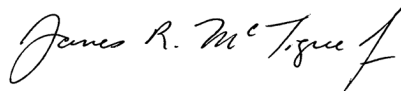
We believe that, given the widespread uncertainty about the FATCA requirements among virtual currency stakeholders, it would benefit taxpayers for IRS to clarify these requirements to the extent possible with the information currently available. It may be appropriate to wait for future

developments in the foreign virtual currency exchange industry before issuing detailed, thorough guidance on this issue. However, IRS could address the uncertainty about the FATCA requirements by clarifying in general terms how it believes they should be interpreted in situations involving virtual currency.

In its comments, FinCEN agreed with the recommendation to make a public statement about whether virtual currency must be reported on the FBAR (recommendation 4). FinCEN confirmed in its letter that as of January 2020, its regulations do not require virtual currency held in an offshore account to be reported on the FBAR. Additionally, FinCEN stated that it will coordinate with IRS to determine the best approach to provide clarity to the public regarding the FBAR requirement.

We are sending copies of this report to the appropriate congressional committees, the Secretary of the Department of the Treasury, the Commissioner of Internal Revenue, the Director of the Financial Crimes Enforcement Network, the Chairman of the Securities and Exchange Commission, the Chairman of the Commodity Futures Trading Commission, and other interested parties. In addition, the report is available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512-9110 or mctiguej@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix IV.



James R. McTigue, Jr.
Director, Tax Issues
Strategic Issues

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) describe what is known about virtual currency tax compliance; (2) describe the steps the Internal Revenue Service (IRS) has taken to address virtual currency tax compliance risks; (3) evaluate the extent to which IRS's virtual currency guidance meets taxpayer needs; and (4) evaluate whether additional information reporting could assist IRS in ensuring compliance.

To describe what is known about virtual currency tax compliance and the steps IRS has taken to address virtual currency tax compliance risks, we reviewed IRS documentation on the agency's virtual currency tax enforcement efforts, including information about the legal summons IRS issued to Coinbase and the Large Business and International (LB&I) division's virtual currency compliance campaign. We interviewed IRS officials in the Small Business/Self Employed (SB/SE) and LB&I operating divisions, as well as the Research, Applied Analytics, and Statistics division about any data the agency had on virtual currency tax compliance, challenges in collecting such data, and plans for data analyses. We also reviewed IRS forms that taxpayers may use to report virtual currency use.

We interviewed officials from the Financial Crimes Enforcement Network, Commodity Futures Trading Commission, and Securities and Exchange Commission about coordination efforts that have been made across agencies regulating virtual currencies. We also interviewed tax practitioners, tax attorneys, virtual currency industry advocates, and virtual currency exchange executives about virtual currency tax compliance issues. We took a snowball sampling approach to identify the outside stakeholders we interviewed, which involved asking stakeholders we interviewed for recommendations of others we should contact to gain additional insight into virtual currency tax compliance, and we assessed their qualifications and independence. In total, we interviewed five individual stakeholders in addition to representatives of 10 entities with expertise in tax issues related to virtual currency. Although results from these interviews are not generalizable, they provide insight into what is known about tax compliance and the steps IRS has taken to address virtual currency tax compliance risks.

To evaluate the extent to which IRS's virtual currency guidance meets taxpayer needs, we identified and analyzed all of the guidance and statements IRS has published about tax compliance for virtual currencies. To identify these documents, we searched IRS's website and interviewed IRS officials. According to IRS officials, Notice 2014-21, issued in March 2014, and Revenue Ruling 2019-24 and Frequently Asked Questions

(FAQs), issued in October 2019, are the only IRS guidance specific to virtual currencies.

We also reviewed and analyzed all of the public comments IRS had received on Notice 2014-21 as of August 19, 2019, to determine the concerns raised about virtual currency tax compliance. IRS sent us 229 public comments. We identified 25 of the comments as not applicable because they were not related to Notice 2014-21, were duplicate comments, or were otherwise not relevant. Two reviewers coded the content of the 204 applicable public comments and grouped them into 13 different thematic categories. We developed these categories based on the topics or issues that commenters identified. We assigned each separate issue raised by a comment to an existing category unless it did not relate to any of the existing categories, in which case we created a new category. We also recorded the date the comment was submitted and the occupation of the commenter, if specified in the comment.

To assess the reliability of these data, we reviewed relevant documentation and consulted knowledgeable IRS officials. Specifically, we requested information from IRS's Office of Chief Counsel to identify the quality controls in place to help ensure all comments are processed. We determined that the data were sufficiently reliable for our purposes. The information we obtained from these comments may not be representative of the viewpoints of the entire U.S. public.

In addition, we interviewed the stakeholders mentioned above before IRS released new guidance in October 2019 to identify any taxpayer concerns, any compliance challenges with virtual currency tax obligations, and the extent to which the guidance provided in IRS's Notice 2014-21 was meeting taxpayer needs. We reached out to these same stakeholders in October 2019, after IRS issued a new set of FAQs and Revenue Ruling 2019-24, to determine how these new guidance documents addressed taxpayers' concerns. Of the five individuals and 10 groups we initially interviewed, we received responses regarding the new IRS guidance from four individuals and six groups. The information we obtained from these practitioners and exchanges is not generalizable to all practitioners and exchanges because we took a snowball sampling approach, but the information provides insight into the extent to which IRS's virtual currency guidance is meeting the needs of taxpayers.

To evaluate whether additional information reporting could assist IRS in ensuring compliance, we reviewed IRS's requirements for information reporting for virtual currency transactions, including the laws and

regulations for foreign asset reporting. We interviewed IRS officials in the SB/SE and LB&I operating divisions about how IRS's third-party and taxpayer information reporting processes and current forms assist in IRS's work to detect noncompliance for virtual currencies. We reviewed the websites of a judgmental selection of nine virtual currency exchanges for policies or statements about tax reporting, including whether the exchanges file Forms 1099-B or 1099-K. For the website review, we selected virtual currency exchanges that were based in the United States and that were likely, because of their size or public profile within the virtual currency industry, to have established policies regarding information reporting. For each exchange, we identified and categorized any statements on the exchange's website regarding tax or information reporting, such as a statement that the exchange does not provide any tax forms to customers or a statement that the exchange provides information on a specific form to customers and IRS.

We also interviewed the stakeholders mentioned above to determine what information is being reported to IRS and whether additional information reporting would help IRS and taxpayers with ensuring tax compliance. We interviewed executives from two exchanges to determine what burden, if any, information reporting does or could impose on exchanges and virtual currency users. We attempted to contact four additional exchanges but did not receive a response. Because we used a snowball sampling approach, the information we obtained from these virtual currency industry participants is not generalizable to all virtual currency industry participants.

We conducted this performance audit from October 2018 to February 2020 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Comments from the Internal Revenue Service



DEPUTY COMMISSIONER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

January 23, 2020

James R. McTigue
Director, Tax Issues
Strategic Issues Team
U.S. Government Accountability Office
441 G Street N.W.
Washington, DC 20548

Dear Mr. McTigue:

Thank you for the opportunity to review and comment on the draft report, *Virtual Currencies: Additional Information Reporting and Clarified Guidance Could Improve Tax Compliance* (GAO-20-188).

As reflected in your report, the IRS has undertaken several measures to address virtual currency tax compliance risks. We continue to engage a broad spectrum of external stakeholders for feedback on how the IRS might balance taxpayer service with proper regulatory enforcement of digital assets, including virtual currency. The wide variety of currency exchanges and digital assets pose a challenge to issuing guidance on specific circumstances, but the guidance issued by the IRS to date illustrates how longstanding tax principles associated with the sale, exchange or disposition of property can apply to virtual currency. We agree that additional information reporting will improve tax compliance and we will continue to engage stakeholders on how this might best be accomplished.

For the 2020 filing season, the IRS has added a new virtual currency question to Schedule 1 of the Form 1040, U.S. Individual Income Tax Return, that will capture sales, receipt, exchanges, or other acquisitions of virtual currency during the tax year. Requiring the reporting of virtual currency events on a tax return is beneficial to both taxpayers (ensures timely and proper treatment of virtual currency transactions) and tax administration (reporting has been shown to increase compliance and minimizes the need to reach out to taxpayers). This effort, coupled with the ongoing enforcement activities through our virtual currency campaign, will enhance voluntary compliance with respect to virtual currencies.

We appreciate GAO's review of this issue. The IRS will remain actively engaged in addressing non-compliance related to virtual currency transactions through a variety of efforts, ranging from taxpayer education to audits to criminal investigations. Virtual currency is an ongoing focus area for IRS Criminal Investigation (IRS-CI). Successful

2

prosecutions of dark web marketplaces, such as 'Welcome To Video' and 'xDedic', as well as other illicit companies like 'OneCoin', continue to deter criminal enterprises from utilizing virtual currency as their primary means of facilitation. Additionally, IRS-CI remains vigilant in the pursuit of stripping nefarious actors of their ill-gotten gains, including virtual currency.

Attached please find our response to the recommendations that are directed to the IRS. If you have any questions, please contact me, or a member of your staff may contact John V. Cardone, Assistant Deputy Commissioner Compliance Integration, Large Business and International Division, at (202) 317-8830.

Sincerely,



Sunita Lough
Deputy Commissioner for
Services and Enforcement

Enclosure

Enclosure

IRS Responses to GAO's Recommendations in the Draft Report on Virtual Currencies:
Additional Information Reporting and Clarified Guidance Could Improve Tax
Compliance (GAO-20-188).

Recommendation 1:

The Commissioner of Internal Revenue should update the FAQs issued in 2019 to include a statement that the FAQs may serve as a source of general information but cannot be relied upon by taxpayers as authoritative since they are not binding on IRS.

Comment:

We disagree with this recommendation. The FAQs are illustrative of how longstanding tax principles apply to property transactions. Further, the IRS does not take positions contrary to public FAQs.

Recommendation 2:

The Commissioner of Internal Revenue should take steps to increase third-party reporting on taxable transactions involving virtual currency, which could include clarifying IRS's interpretation of existing third-party reporting requirements under the Internal Revenue Code and Treasury Regulations, or pursuing statutory or regulatory changes.

Comment:

We agree with this recommendation. One of the items on the Department of the Treasury 2019-2020 Priority Guidance Plan is "Guidance regarding information reporting on virtual currency under §6045." IRS Office of Chief Counsel and the Department of Treasury are working on guidance that will address third-party reporting under section 6045 on certain taxable transactions involving virtual currency. It is anticipated that the guidance will also propose rules to avoid duplicate reporting under other information reporting regimes that may apply to transactions involving virtual currency.

Recommendation 3:

The Commissioner of Internal Revenue should clarify the application of reporting requirements under the Foreign Account Tax Compliance Act to virtual currency.

Comment:

We disagree with this recommendation. It is appropriate at this time to focus guidance on information reporting on transactions subject to section 6045, in light of the significant role that U.S. exchanges and other U.S. businesses play in virtual currency transactions carried out by U.S. taxpayers. As the workings of foreign virtual currency exchanges become more transparent over time, additional FATCA guidance may be appropriate in the future.

Appendix III: Comments from the Financial Crimes Enforcement Network



Financial Crimes Enforcement Network
U.S. Department of the Treasury

Office of the Director

Washington, D.C. 20220

January 22, 2020

James R. McTigue, Jr.
Director, Tax Issues
Strategic Issues
United States Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. McTigue:

Thank you for providing the Financial Crimes Enforcement Network (FinCEN) the opportunity to review the Government Accountability Office (GAO) report, "Virtual Currencies, Additional Information Reporting and Clarified Guidance Could Improve Tax Compliance (GAO- 20-188)." FinCEN supports your objective to determine if additional information reporting and guidance can improve tax compliance as it relates to virtual currencies. FinCEN concurs with Recommendation Four set out in the report and which states that "[t]he Director of FinCEN, in coordination with IRS as appropriate, should make a statement about the application of foreign account reporting requirements under the Bank Secrecy Act to virtual currency readily available to the public."

FinCEN will coordinate with the IRS to determine the best approach to provide clarity to the public regarding the application of the Report of Foreign Bank and Financial Accounts (FBAR) to virtual currency. Currently, the FBAR regulations do not define virtual currency held in an offshore account as a type of reportable account. (See 31 CFR 1010.350(c)). For that reason, at this time, virtual currency held in an offshore account is not reportable on the FBAR. FinCEN, however, in consultation with the IRS, continues to evaluate the value of incorporating virtual currency held offshore into the FBAR regulatory reporting requirements.

We appreciate the role of the GAO in providing oversight of our programs and look forward to working with GAO in the future.

Sincerely,

/s/

Kenneth A. Blanco
Director

www.fincen.gov

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact:

James R. McTigue, Jr. (202) 512-9110, mctiguej@gao.gov

Staff Acknowledgments

In addition to the contact named above, Jeff Arkin (Assistant Director), Danielle Novak (Analyst-in-Charge), Theodore Alexander, Michael Bechetti, David Blanding, Jacqueline Chapin, Ed Nannenhorn, Bruna Oliveira, Kayla Robinson, and Andrew J. Stephens made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its [website](#) newly released reports, testimony, and correspondence. You can also [subscribe](#) to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <https://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#).
Subscribe to our [RSS Feeds](#) or [Email Updates](#). Listen to our [Podcasts](#).
Visit GAO on the web at <https://www.gao.gov>.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: <https://www.gao.gov/fraudnet/fraudnet.htm>

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548





11/11/2020

RESEARCH, APPLIED ANALYTICS & STATISTICS (RAAS)
STATISTICS OF INCOME (SOI), STATISTICAL SERVICES BRANCH

Comprehensive Taxpayer Attitude Survey (CTAS) 2020 Executive Report

Table of Contents

Background..... 3

Summary Findings and Recommendations..... 6

Taxpayer Relationship to Tax Obligations13

Factors Influencing Taxpayer Compliance.....27

Sources of Tax Information and Advice.....32

IRS Services Provided to Taxpayers40

Background

Study Objectives

The objectives of the CTAS research study are to:

- Provide greater insights into tax compliance attitudes, customer service satisfaction, and preferences.
- Identify trends that may signal a change in attitudes or behaviors.
- Track both online and RDD phone responses to maintain historical trending, while evaluating differences in data and sampling across modes.
- Annually, adjust questionnaire to capture emerging trends and to streamline the survey for maximum efficiency.

Methodology

Pacific Consulting Group (PCG) fielded the 2020 Comprehensive Taxpayer Attitude Survey (CTAS) from August 24 – September 24, 2020, collecting a total of 2,017 surveys from the general public.*

- PCG employed a multi-mode data collection methodology, comprised of telephone and online random sampling, to ensure a representative sample of U.S. adults, aged 18 or over.
 - A total of 1,000 telephone survey responses were collected via random digit dialing (RDD) to households with landlines in the continental U.S. (500 interviews) and to cell phone numbers (500 interviews). The interviewing methodology used was Computer Assisted Telephone Interviewing (CATI).
 - A total of 1,017 online survey responses were collected. PCG subcontracted with Ipsos to provide the online sample from their probability based online panel, KnowledgePanel®. This panel uses an Address-Based Sampling (ABS) methodology, which randomly recruits members by mail.
- The response rate (total # completed interviews/total # contacts) was 2.4% for phone survey and 62.8% for online survey. The average interview length was 27.57 minutes for phone and 14.5 minutes for online survey.
- Survey data from each data collection mode were weighted separately to allow for analysis of each sample separately and comparatively. The phone and online samples were also combined by generating an additional ‘blended’ weight variable.

* Margin of error: +/- 2.1% at 95% confidence level.

Summary Findings and Recommendations

Taxpayers continue to believe in individual compliance

- Similar to previous years, the majority of taxpayers feel it is 'not at all' acceptable to cheat on taxes (87%), that it is every American's civic duty to pay their fair share of taxes (94% agree), and that everyone who cheats on their taxes should be held accountable (91% agree). Older Americans tend to be even stronger believers than their younger counterparts.
- However, less than half of taxpayers (47%) agree it is their personal responsibility to report anyone who cheats on taxes.
- Taxpayers' trust in the IRS to fairly enforce the tax laws and to help taxpayers understand their tax obligations were at parity with last year, while their trust in the IRS to protect their tax account records from cyber criminals significantly increased.
- Yet, overall there are some taxpayers that do not trust the IRS; in fact a third 'completely' or 'mostly disagree' that they trust the IRS to help them understand their obligations. Across all areas tested, trust is especially lower among younger taxpayers, those that are more educated, and taxpayers with higher income.
- Whether filing a tax return or actually speaking with an IRS representative, most taxpayers are satisfied (78%) with their personal interactions with the IRS and levels have remained steady since 2017.

The greatest factor influencing taxpayer compliance is *personal integrity*; however, compliance drivers differ among demographics

- Personal integrity is ‘a great deal’ or ‘somewhat’ of an influence to report and pay taxes honestly for 92% of taxpayers, followed by avoiding interest/penalties (77%), and their ability to pay (68%).
- Compared to older generations, millennials are significantly more influenced by the threat of paying interest/penalties, their ability to pay, fear of an audit, and how the government uses the taxes.
- Overall, less educated taxpayers are more influenced by their ability to pay and the option to pay in installments. However, high school-only educated taxpayers are significantly more influenced by the belief that their neighbors are reporting and paying honestly (40%) versus those with some college or a degree (33% and 32%, respectively).
- Those with the highest income are less influenced by outside measures; personal integrity is their top driver (95%) to report and pay honestly.

The IRS website and tax professionals continue to be the most valuable sources for tax advice/information

- The most valuable sources of getting tax advice and information are the IRS website (88%), paid tax professionals (88%), IRS representatives (85%), and an IRS personal online account (84%).
- IRS printed publications (78%), IRS applications on mobile devices (69%), reference materials from sources other than the IRS (68%), family and friends (59%) and IRS tax sources on social media (45%) are viewed as the least valuable. However, online and mobile sources show more variation by age, with younger taxpayers finding them more valuable than older. Additionally, friends or family are especially valuable to those 18-24 years.
- 34% of taxpayers contacted the IRS at some point over the past year. The IRS website and the toll-free number were the most used methods of initiating contact with the IRS in the last year, excluding the filing of tax returns (22% and 13%, respectively).
- Half of taxpayers used a paid tax professional. Usage of a paid tax professional increases with age and income.

Taxpayers believe additional IRS help will promote increased return accuracy and believe online and toll-free services are the most important channels for assistance

- Taxpayers agree that the more information and guidance the IRS provides, the more likely people are to correctly file their tax returns (90% agree).
- 36% of taxpayers tend to believe that the IRS devotes too much of its resources to enforcement activities and not enough to its customer service programs, while 46% indicate that the IRS maintains a proper balance. Only 10% of taxpayers feel that the IRS devotes *too much* of its resources to customer service.
- When it comes to services, taxpayers feel it's most important that the IRS provides opportunities to file taxes electronically (93%), information on their website (90%), and a toll-free number to answer questions (86%).
- The importance of the IRS offering in-person services significantly decreased in 2020 versus previous years. Significantly fewer taxpayers agreed that it is important for the IRS to provide office locations with an onsite IRS representative (76% agree vs. 85% in 2019) or community-based tax clinics at convenient locations (71% agree vs. 79% in 2019).
- Yet, the share of taxpayers who agree the IRS should focus on improving in-person and phone call assistance to taxpayers continues to increase (86% agree vs. 70% in 2019).

Recommendations: Actions to Improve Taxpayer Compliance

- ✓ To improve taxpayer compliance:
 - ✓ Look for opportunities to tailor messaging and channels as appropriate to the various demographics:
 - ✓ For millennials, provide easy to digest, relevant information on how the government uses taxes. Consider outlining how much money was paid in interest and penalties the previous year in order to emphasize one of their most influential factors to report/pay honestly and further bring the consequences to life.
 - ✓ For college-educated and high-income taxpayers, explore opportunities in messaging and campaigns to further connect the action of accurately reporting/paying taxes with personal integrity.
 - ✓ For taxpayers with less schooling, focus on building awareness and education regarding payment programs/options. Additionally, consider ways to emphasize and localize the percentage of taxpayers near them that report and pay honestly (i.e. Did you know that in the XXXXX zip code 98% of your neighbors reported and paid accurately?).

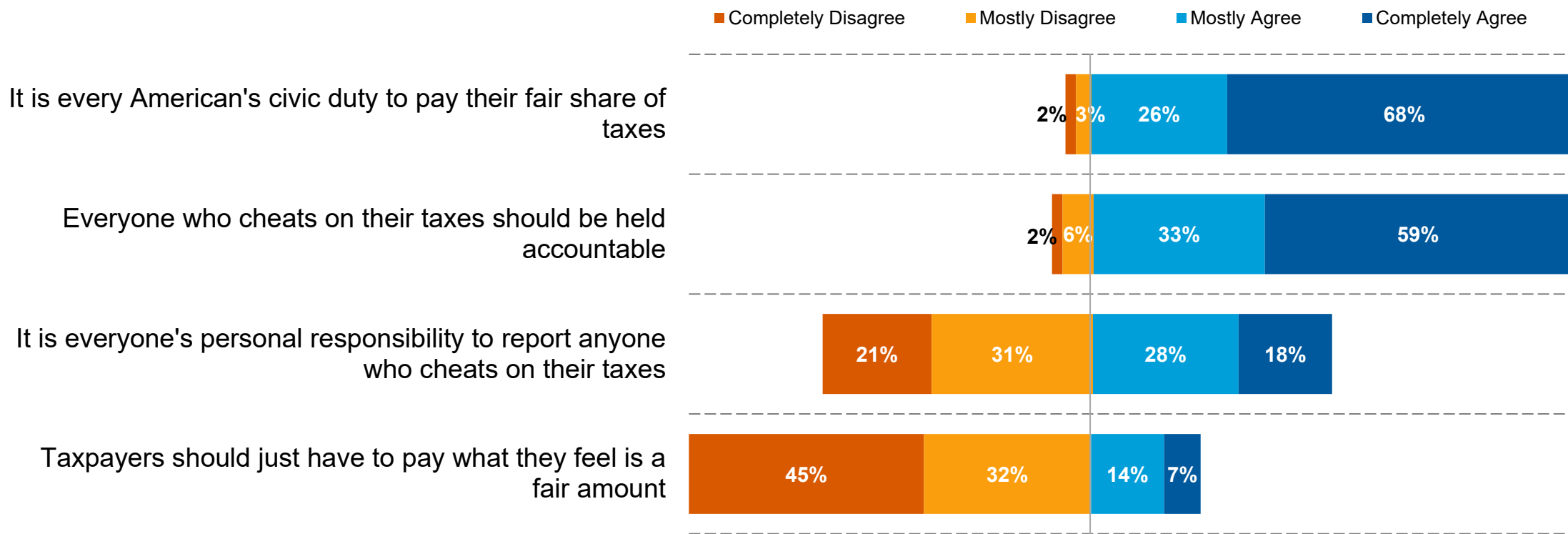
Recommendations: Actions to Improve Taxpayers' Trust and Experience with the IRS

- ✓ To maintain and grow taxpayers' trust and perception of the IRS:
 - ✓ Make taxpayers aware of how much the IRS helps and successfully interacts with taxpayers each year. Highlight data that conveys commitment and customer service-dedicated resources (number of taxpayer calls fielded in 2020, hours spent assisting with returns, etc.).
- ✓ To improve taxpayers' experience:
 - ✓ Funnel resources towards improving IRS online platforms (website/online accounts/email) and 'live remote' (toll-free number) experiences. Deprioritize improvements of in-person services.
 - ✓ Leverage the higher interest in online channels and proactively market those channels to promote adoption.

Taxpayer Relationship to Tax Obligations

Most view taxes as a civic duty and feel those who cheat should be held accountable; however, personal responsibility to report cheaters is polarized

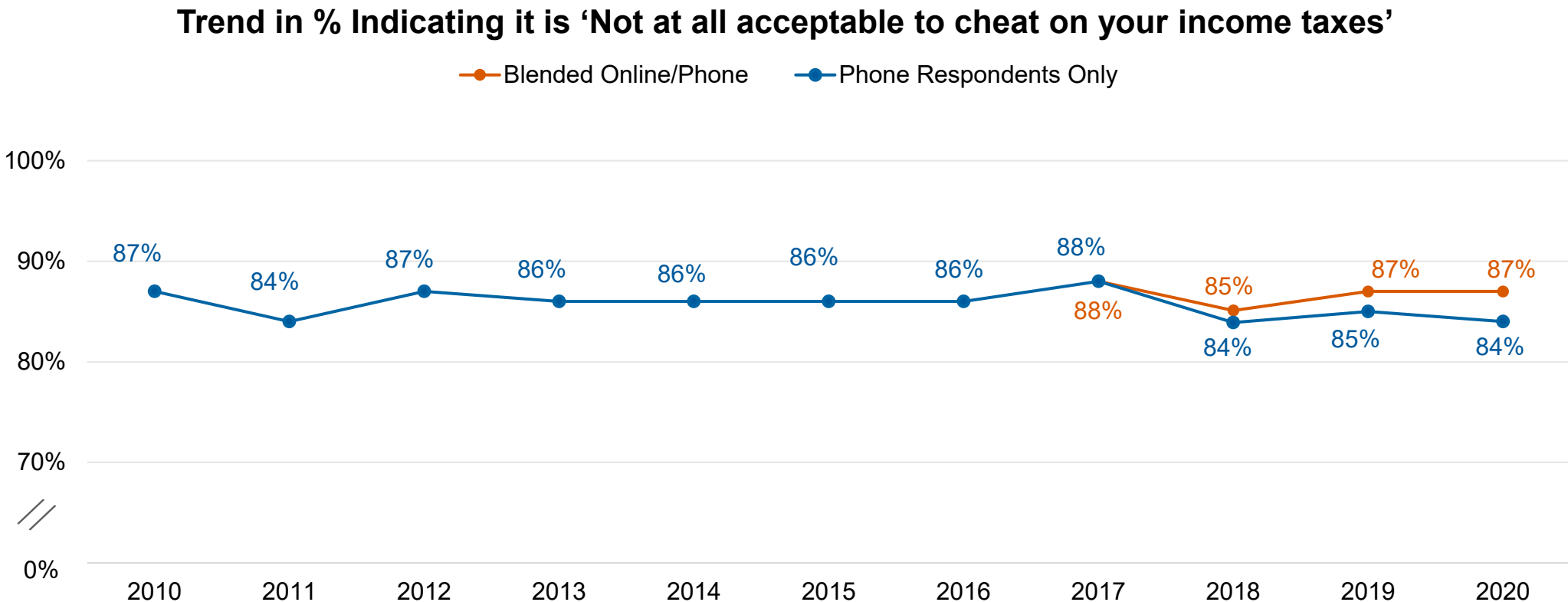
Attitudes about Cheating and Payment of Fair Share of Taxes



Q2: For each of the following statements, please indicate whether you completely agree, mostly agree, mostly disagree, or completely disagree.

Margin of error is +/- 2.1% for blended online/phone respondents. Note: Each stacked bar may not add up to 100% due to "don't know," "not applicable," or "no response."

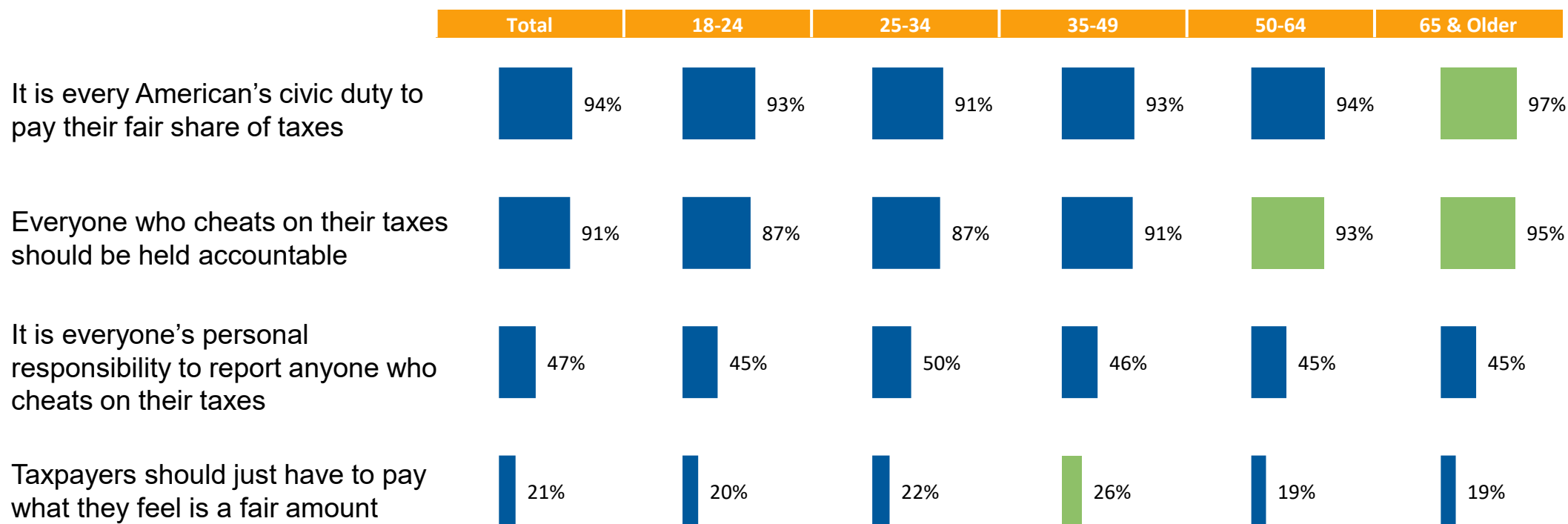
Taxpayers continue to have an ethical attitude about not cheating on their income taxes, with over 8 in 10 stating it is ‘not at all acceptable’



Q1: How much, if any, do you think is an acceptable amount to cheat on your income taxes? Would you say...?
Margin of error is +/- 2.1% for blended online/phone respondents and +/- 3.1% for phone respondents only.

Older taxpayers are significantly more likely to agree that taxes are a civic duty and everyone that cheats should be held accountable

% Agreement: Attitudes about Cheating and Payment of Fair Share of Taxes by Age

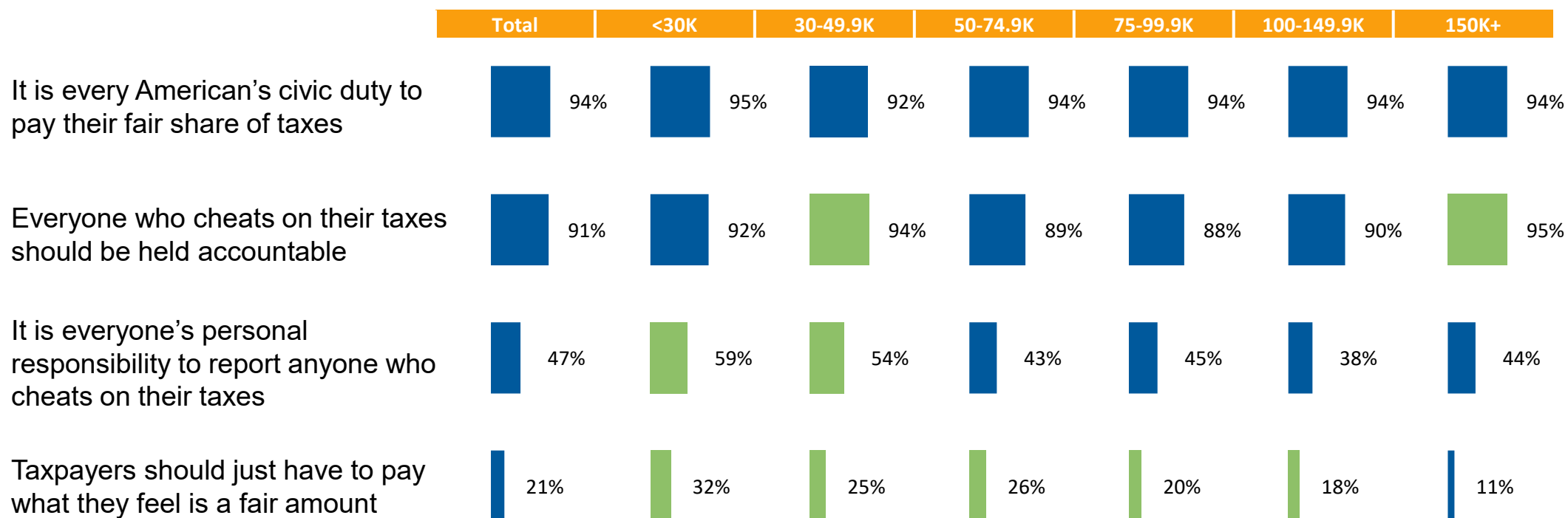


Q2: For each of the following statements, please indicate whether you completely agree, mostly agree, mostly disagree, or completely disagree.

Margin of error is +/- 2.1% for blended online/phone respondents. Percentage 'completely agree' plus 'mostly agree' is shown. **Lighter green shading** indicates a significantly higher score at a 95% confidence level versus other scores in the row.

Likewise, taxpayers in the highest income bracket are significantly more likely to agree everyone that cheats should be held accountable

% Agreement: Attitudes about Cheating and Payment of Fair Share of Taxes by Income



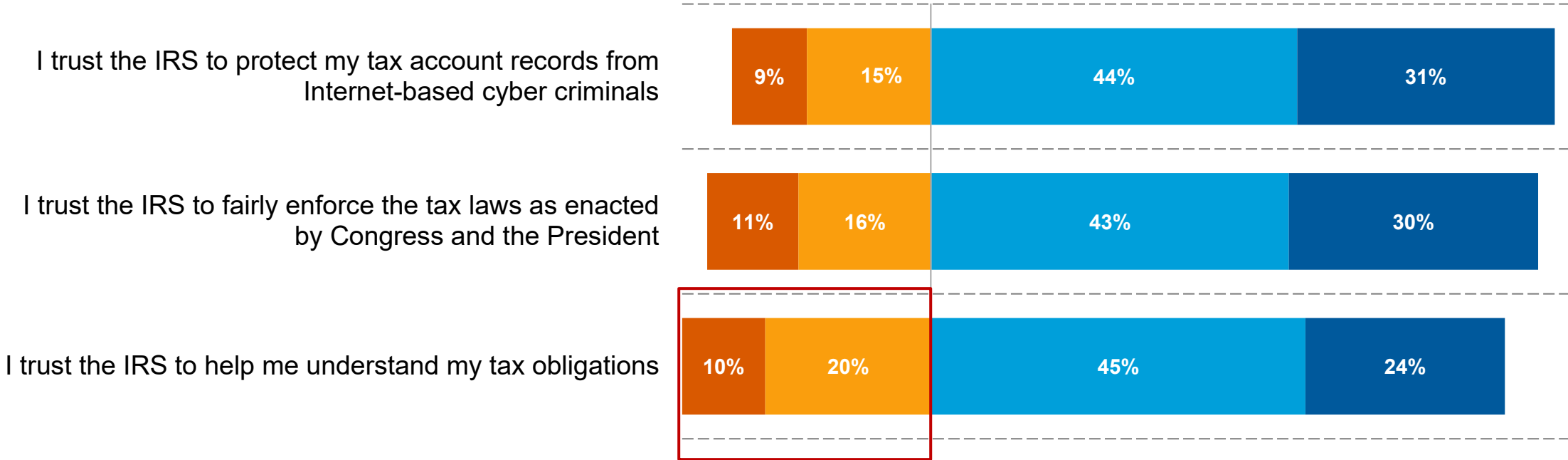
Q2: For each of the following statements, please indicate whether you completely agree, mostly agree, mostly disagree, or completely disagree.

Margin of error is +/- 2.1% for blended online/phone respondents. Percentage 'completely agree' plus 'mostly agree' is shown. Lighter green shading indicates a significantly higher score at a 95% confidence level versus other scores in the row.

Taxpayers' trust of the IRS remains relatively high and mostly at parity with 2019; the biggest opportunity for improvement is helping taxpayers understand their obligations

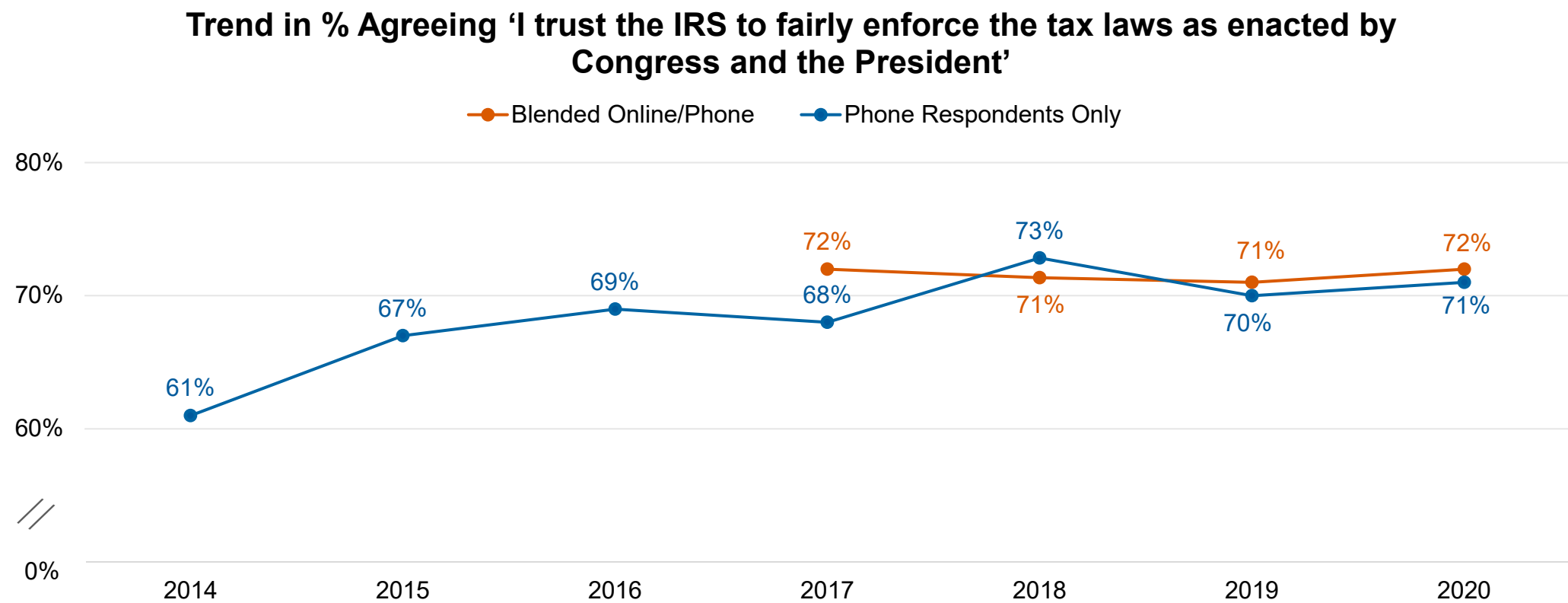
Trust in the IRS

■ Completely Disagree ■ Mostly Disagree ■ Mostly Agree ■ Completely Agree



Q2: For each of the following statements, please indicate whether you completely agree, mostly agree, mostly disagree, or completely disagree.
Margin of error is +/- 2.1% for blended online/phone respondents. Note: Each stacked bar may not add up to 100% due to “don’t know,” “not applicable,” or “no response.”

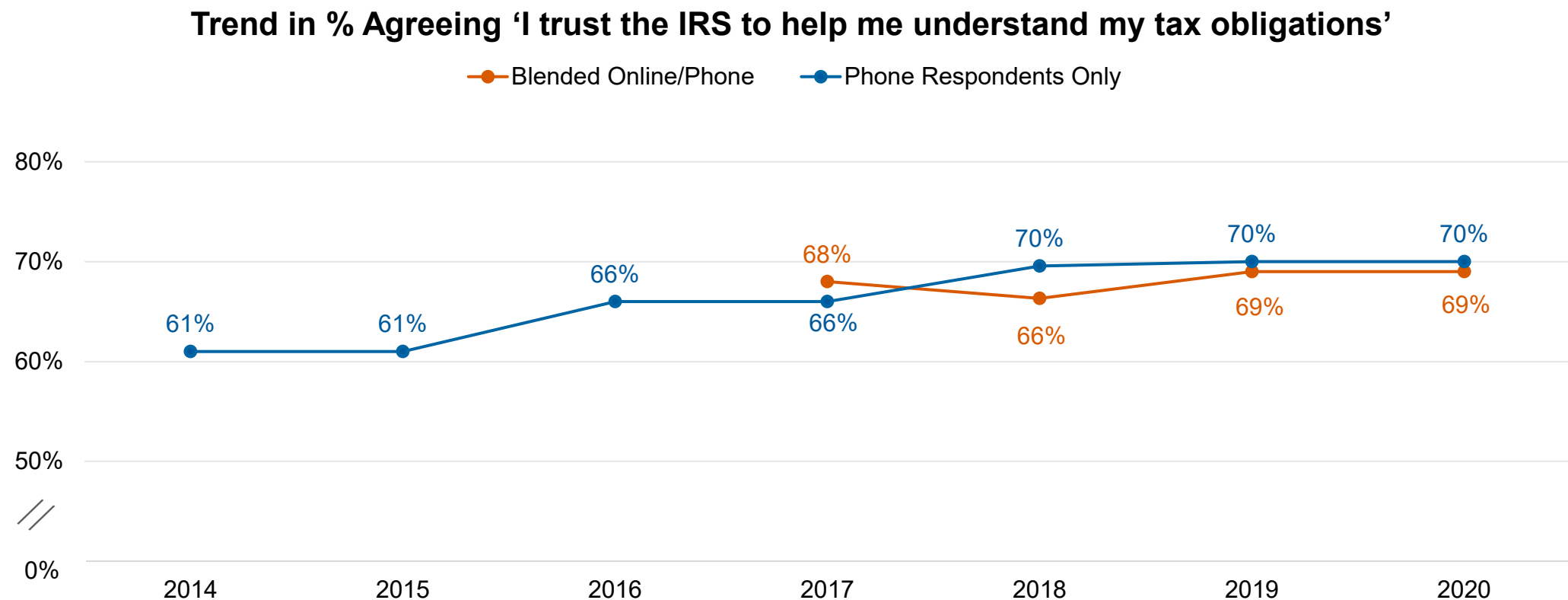
The percentage who agree that they trust the IRS to fairly enforce tax laws has continued to trend up



Q2: For each of the following statements, please indicate whether you completely agree, mostly agree, mostly disagree, or completely disagree. Percentage 'completely agree' plus 'mostly agree' is shown.

Margin of error is +/- 2.1% for blended online/phone respondents and +/- 3.1% for phone respondents only.

The percentage agreeing that they trust the IRS to help understand their tax obligations remained the same versus 2019

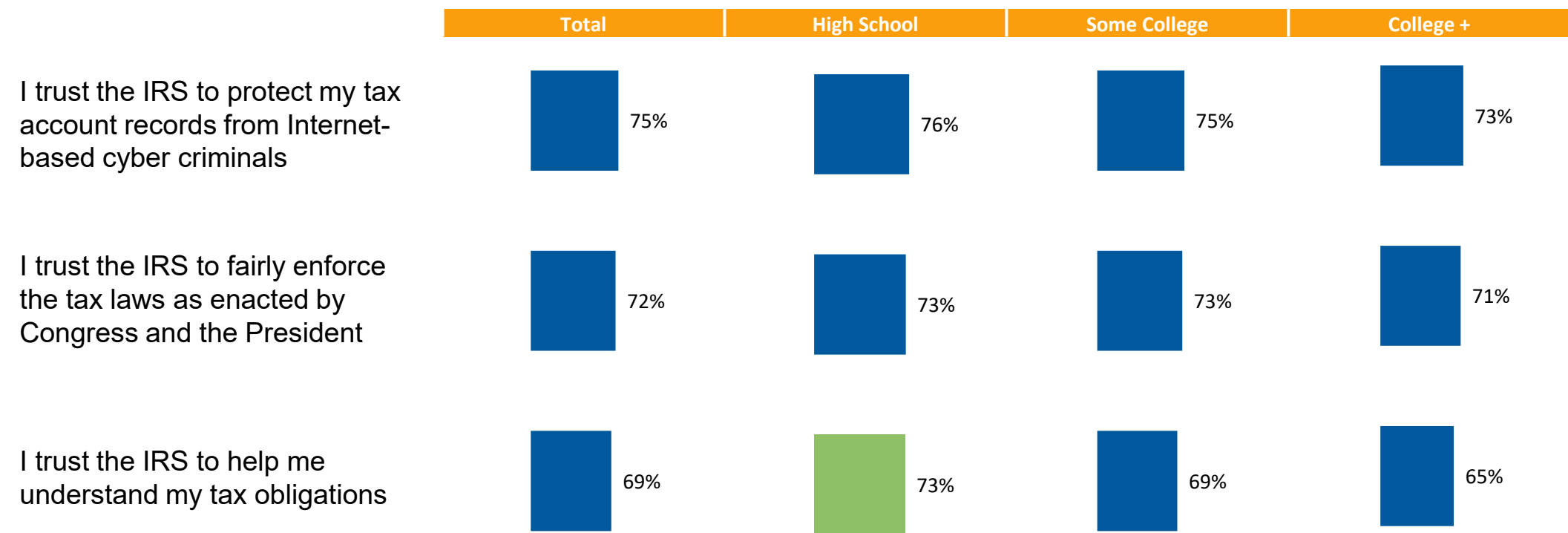


Q2: For each of the following statements, please indicate whether you completely agree, mostly agree, mostly disagree, or completely disagree. Percentage ‘completely agree’ plus ‘mostly agree’ is shown.

Margin of error is +/- 2.1% for blended online/phone respondents and +/- 3.1% for phone respondents only.

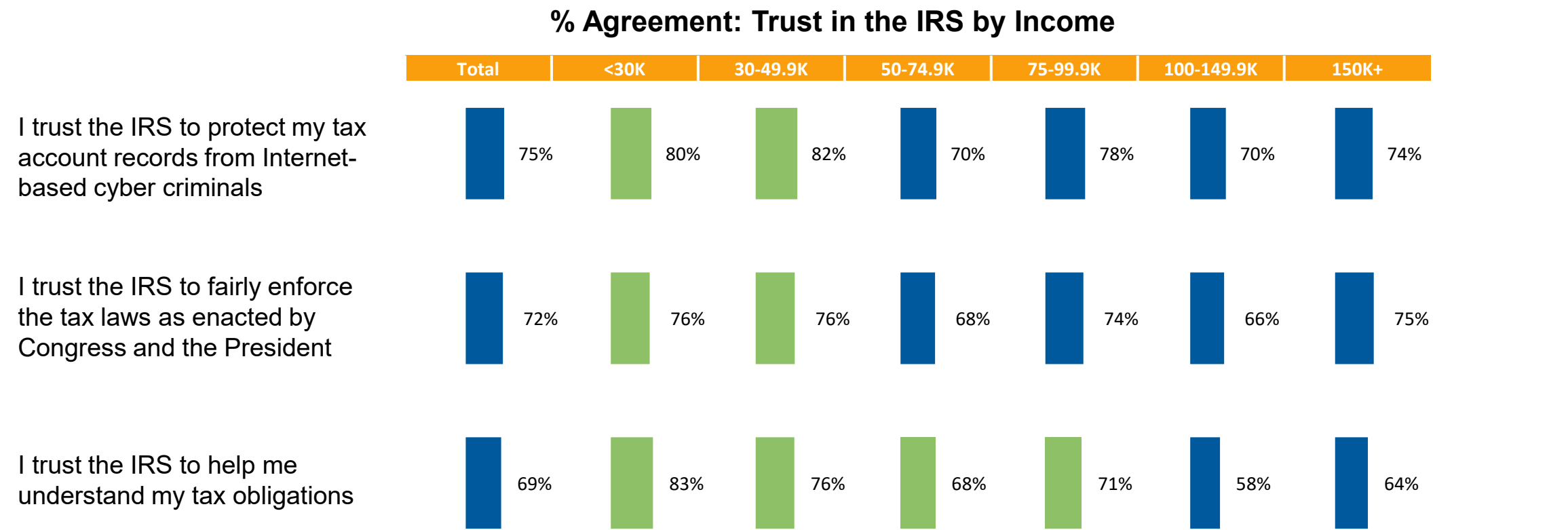
Trust is directionally lower among more educated taxpayers; those with a high school education are significantly more likely to trust the IRS to help them with their tax obligations than the college-educated

% Agreement: Trust in the IRS by Education



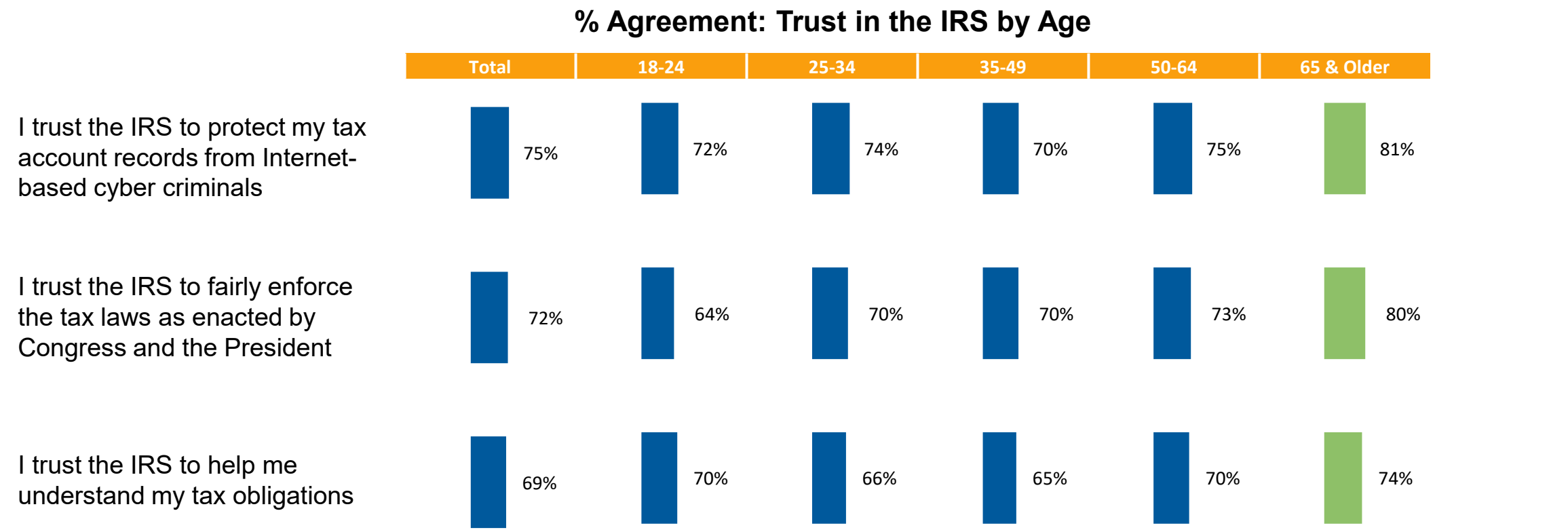
Q2: For each of the following statements, please indicate whether you completely agree, mostly agree, mostly disagree, or completely disagree. Margin of error is +/- 2.1% for blended online/phone respondents. Percentage 'completely agree' plus 'mostly agree' is shown. Lighter green shading indicates a significantly higher score at a 95% confidence level versus other scores in the row.

Taxpayers in the lower income brackets are significantly more trusting of the IRS to protect records, enforce the tax laws, and help them understand their obligations



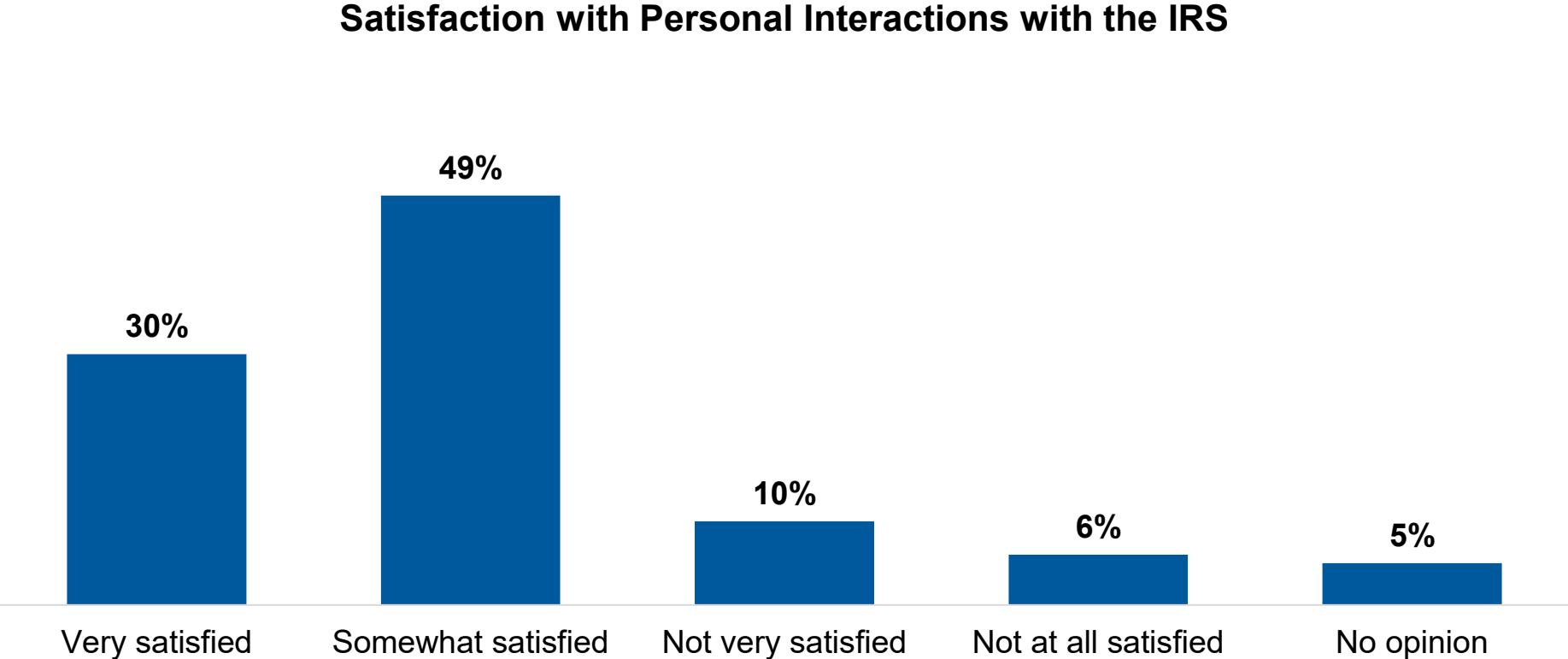
Q2: For each of the following statements, please indicate whether you completely agree, mostly agree, mostly disagree, or completely disagree. Margin of error is +/- 2.1% for blended online/phone respondents. Percentage 'completely agree' plus 'mostly agree' is shown. **Lighter green shading** indicates a significantly higher score at a 95% confidence level versus other scores in the row.

Trust is higher among older taxpayers; those 65 and older are significantly more likely to trust the IRS across all areas compared to some of their younger counterparts



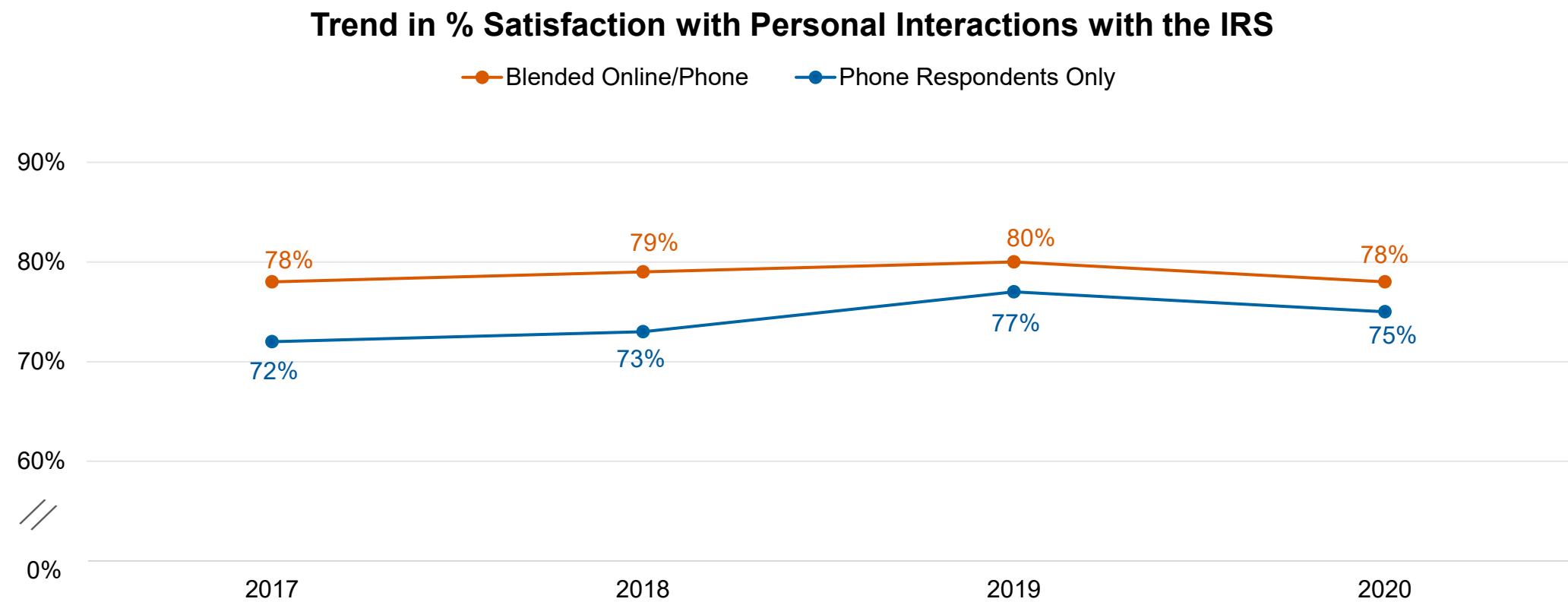
Q2: For each of the following statements, please indicate whether you completely agree, mostly agree, mostly disagree, or completely disagree.
Margin of error is +/- 2.1% for blended online/phone respondents. Percentage 'completely agree' plus 'mostly agree' is shown. **Lighter green shading** indicates a significantly higher score at a 95% confidence level versus other scores in the row.

Most taxpayers are satisfied with their personal interactions with the IRS



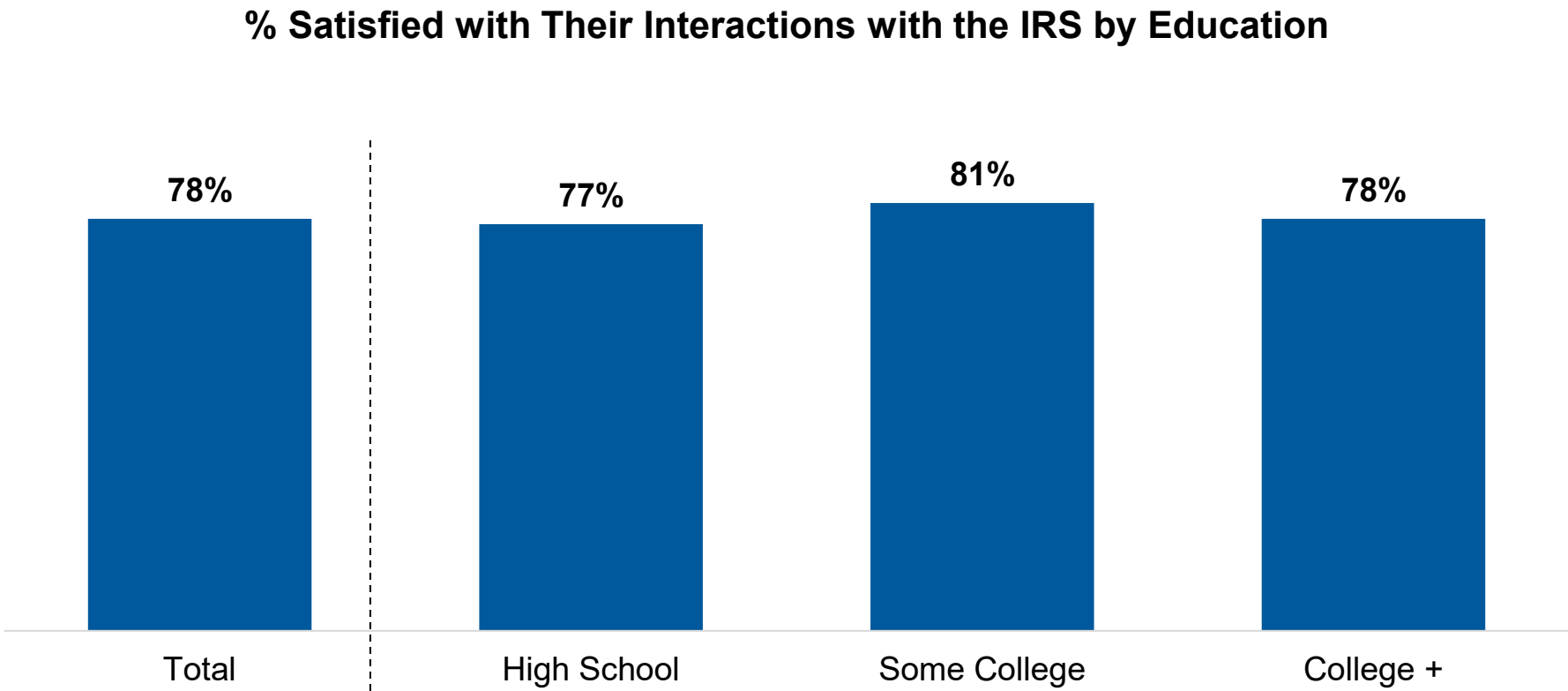
Q10: How satisfied would you say you have been with your personal interaction with the IRS? Would you say very satisfied, somewhat satisfied, not very satisfied, or not at all satisfied?
Margin of error is +/- 2.1% for blended online/phone respondents.

Satisfaction with personal interactions with the IRS has remained steady since 2017



Q10: How satisfied would you say you have been with your personal interaction with the IRS? Would you say very satisfied, somewhat satisfied, not very satisfied, or not at all satisfied?
Percentage of 'very satisfied' plus 'somewhat satisfied' is shown.
Margin of error is +/- 2.1% for blended online/phone respondents and +/- 3.1% for phone respondents only.

Satisfaction is at parity among education levels

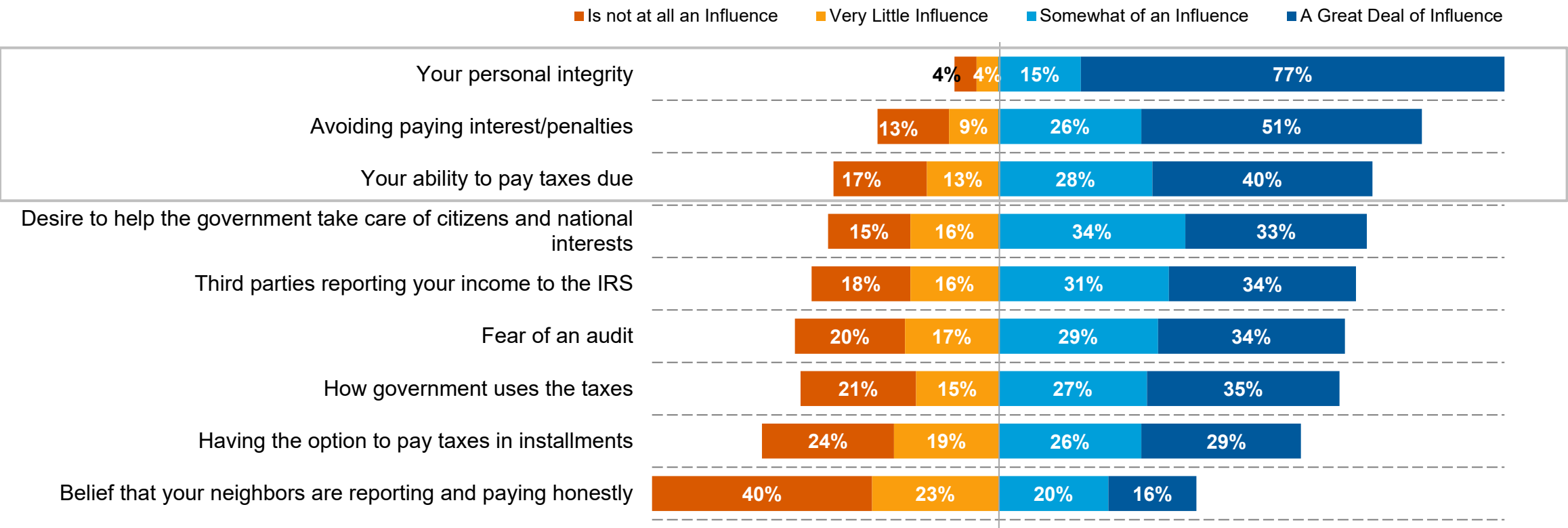


Q10: How satisfied would you say you have been with your personal interaction with the IRS? Would you say very satisfied, somewhat satisfied, not very satisfied, or not at all satisfied? Percentage 'very satisfied' plus 'somewhat satisfied' is shown.
Margin of error is +/- 2.1% for blended online/phone respondents.

Factors Influencing Taxpayer Compliance

The greatest influences on taxpayers to report and pay honestly are personal integrity, to avoid paying interest / penalties, and their overall ability to pay

Influence of Factors In Reporting and Paying Taxes Honestly



Q4: How much influence does each of the following factors have on whether you report and pay your taxes honestly? Would you say it has a great deal of influence, somewhat of an influence, very little influence, or is not at all an influence?

Margin of error is +/- 2.1% for blended online/phone respondents. Note: Each stacked bar may not add up to 100% due to “don’t know,” “not applicable,” or “no response.”

Compared to older generations, millennials are significantly more influenced by avoiding penalties, their ability to pay, fear of an audit, and how the government uses the taxes

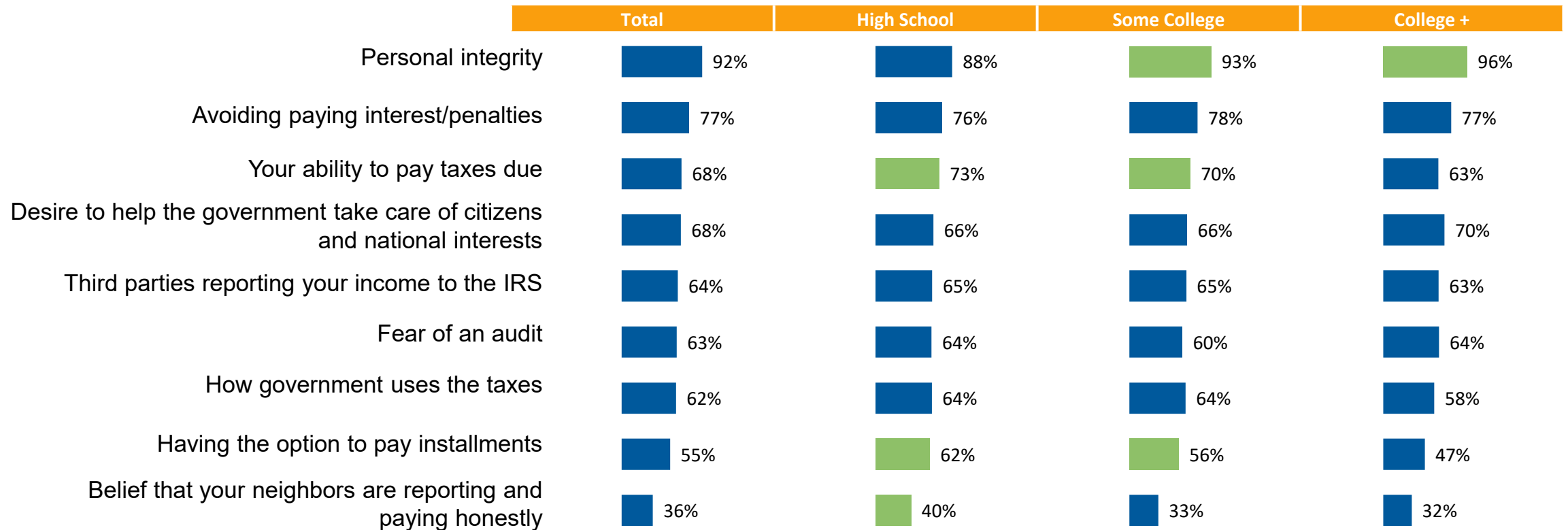
% Influenced: Factors In Reporting and Paying Taxes Honestly by Age

	Total	18-24	25-34	35-49	50-64	65 & Older
Personal integrity	92%	88%	91%	94%	94%	91%
Avoiding paying interest/penalties	77%	84%	79%	77%	77%	73%
Your ability to pay taxes due	68%	78%	71%	68%	67%	63%
Desire to help the government take care of citizens and national interests	68%	66%	68%	66%	67%	69%
Third parties reporting your income to the IRS	64%	73%	65%	62%	65%	62%
Fear of an audit	63%	72%	73%	64%	62%	50%
How government uses the taxes	62%	72%	64%	64%	56%	61%
Having the option to pay installments	55%	62%	51%	53%	57%	57%
Belief that your neighbors are reporting and paying honestly	36%	41%	34%	36%	33%	37%

Q4: How much influence does each of the following factors have on whether you report and pay your taxes honestly? Would you say it has a great deal of influence, somewhat of an influence, very little influence, or is not at all an influence? Margin of error is +/- 2.1% for blended online/phone respondents. Percentage of 'somewhat of an influence' and 'great influence' is shown. **Lighter green shading** indicates a significantly higher score at a 95% confidence level versus other scores in the row.

Less educated taxpayers are more influenced by their ability to pay and paying in installments versus their college+ counterparts; high school grads are significantly more influenced by the belief their peers are acting honestly

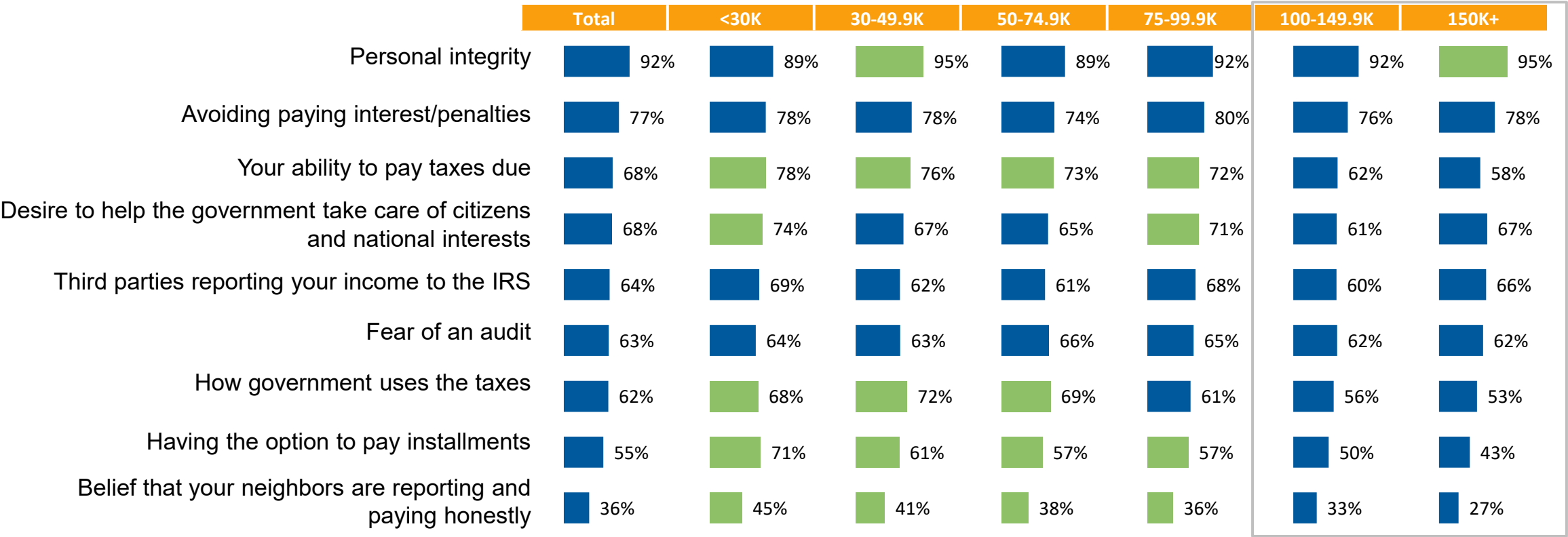
% Influenced: Factors In Reporting and Paying Taxes Honestly by Education



Q4: How much influence does each of the following factors have on whether you report and pay your taxes honestly? Would you say it has a great deal of influence, somewhat of an influence, very little influence, or is not at all an influence? Margin of error is +/- 2.1% for blended online/phone respondents. Percentage of 'somewhat of an influence' and 'great influence' is shown. **Lighter green shading** indicates a significantly higher score at a 95% confidence level versus other scores in the row.

Those with the highest income are overall less influenced by outside measures; personal integrity is their top driver to report and pay honestly

% Influenced: Factors In Reporting and Paying Taxes Honestly by Income

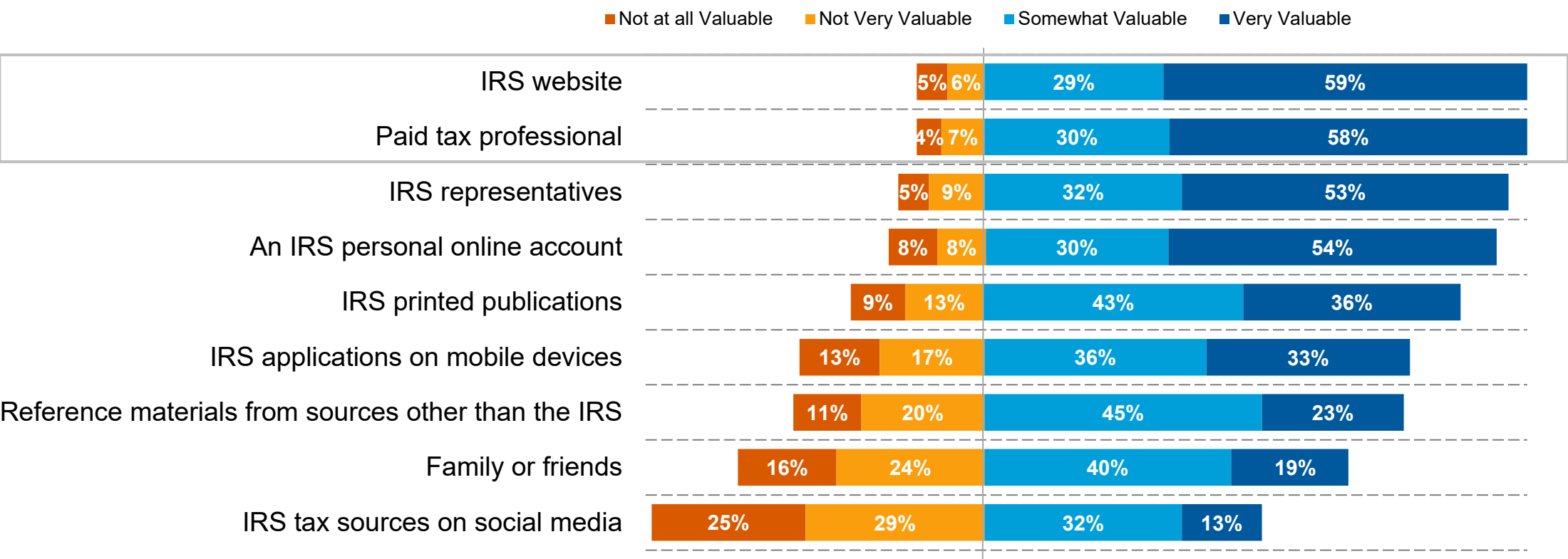


Q4: How much influence does each of the following factors have on whether you report and pay your taxes honestly? Would you say it has a great deal of influence, somewhat of an influence, very little influence, or is not at all an influence? Margin of error is +/- 2.1% for blended online/phone respondents. Percentage of 'somewhat of an influence' and 'great influence' is shown. **Lighter green shading** indicates a significantly higher score at a 95% confidence level versus other scores in the row.

Sources of Tax Information and Advice

The IRS website and tax professionals continue to be the most valuable sources for tax advice/information

Value of Sources of Getting Tax Advice or Information



Q9: How valuable would you say each of these sources is for getting tax advice or information? Would you say it is very valuable, somewhat valuable, not very valuable, or not at all valuable? Margin of error is +/- 2.1% for blended online/phone respondents. Note: Each stacked bar may not add up to 100% due to “don’t know,” “not applicable,” or “no response.”

Online and mobile sources show more variation by age with younger taxpayers finding them more valuable than older; friends and family are especially valuable to those who are 18-24 years old

% Valuable: Source of Tax Advice by Age

	Total	18-24	25-34	35-49	50-64	65 & Older
IRS Website	88%	95%	90%	90%	91%	79%
Paid tax professional	88%	91%	89%	88%	87%	88%
IRS representatives	85%	88%	87%	84%	87%	83%
An IRS personal online account	84%	95%	93%	86%	84%	68%
IRS printed publications	78%	78%	80%	72%	82%	79%
IRS applications on mobile devices	69%	86%	81%	76%	65%	49%
Reference materials from sources other than the IRS	68%	79%	73%	74%	67%	56%
Family or friends	59%	82%	68%	65%	52%	45%
IRS tax sources on social media	45%	63%	53%	46%	43%	33%

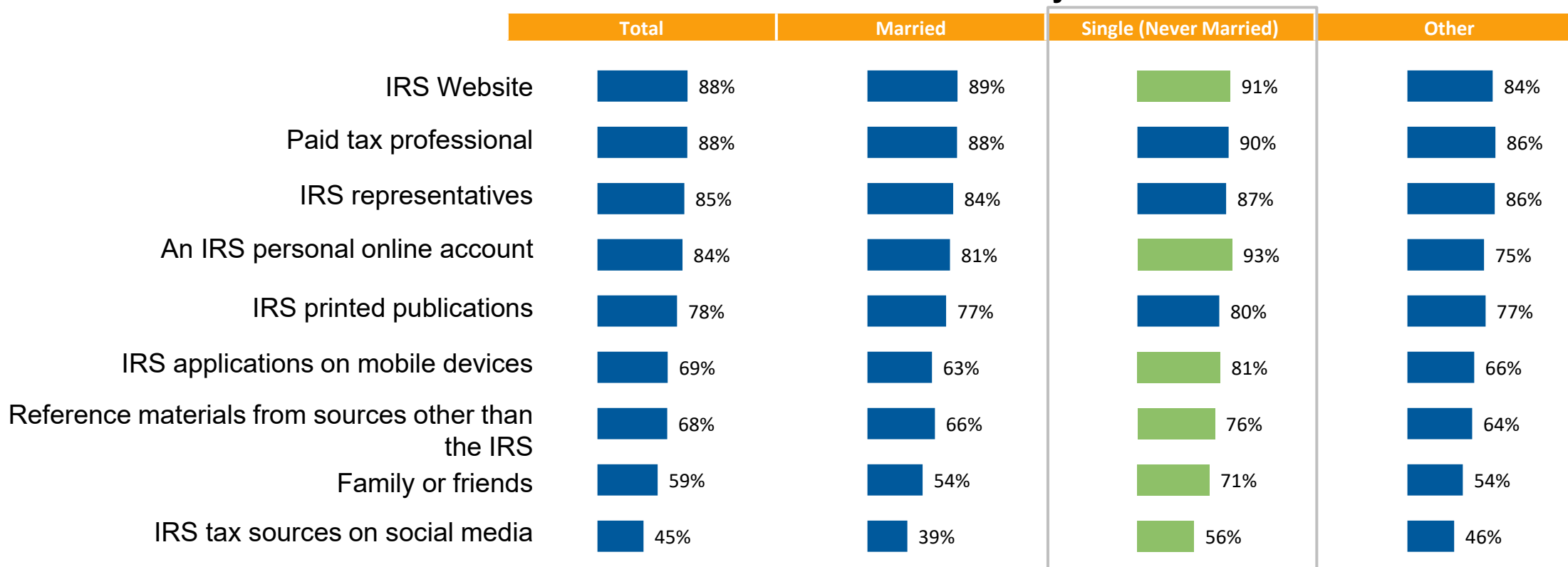
Q9: How valuable would you say each of these sources is for getting tax advice or information? Would you say it is very valuable, somewhat valuable, not very valuable, or not at all valuable?

Percentage of 'very valuable' plus 'somewhat valuable' is shown.

Margin of error is +/- 2.1% for blended online/phone respondents. Lighter green shading indicates a significantly higher score at a 95% confidence level versus other scores in the row.

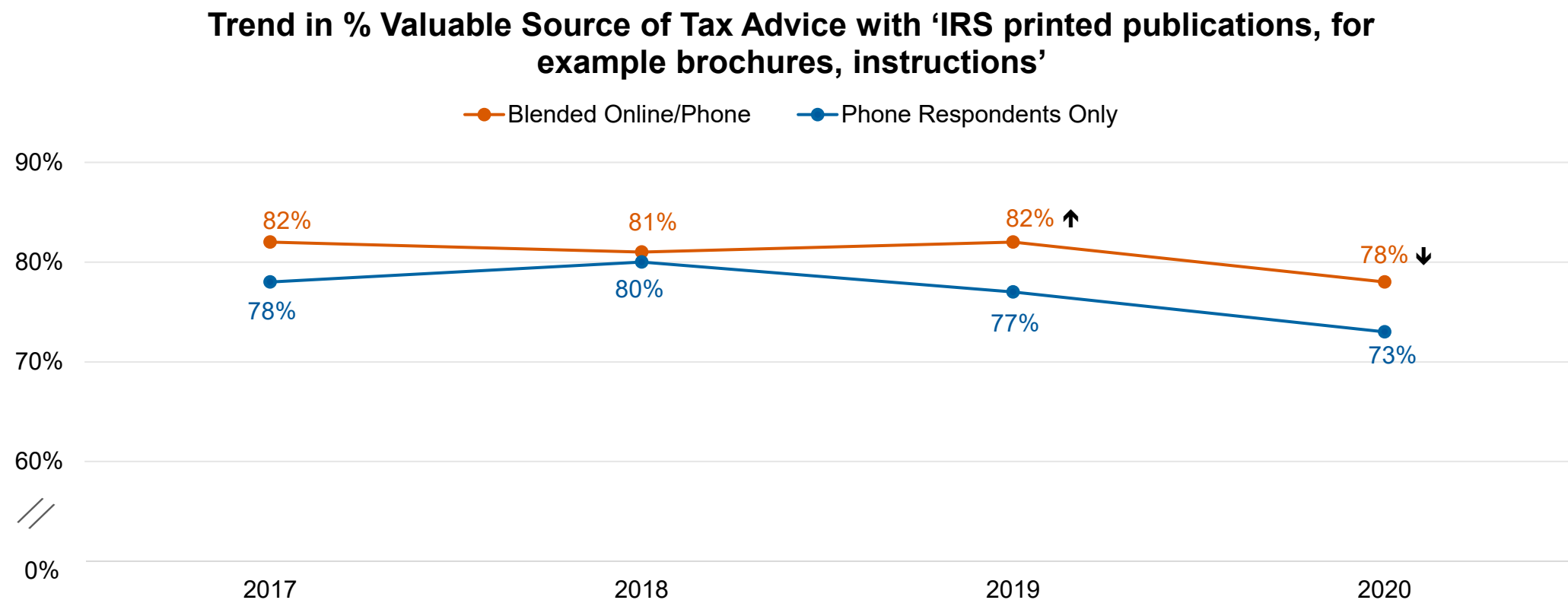
Single (never married) taxpayers find most tax advice sources significantly more valuable than those who are married or fall under 'other'

% Valuable: Source of Tax Advice by Marital Status



Q9: How valuable would you say each of these sources is for getting tax advice or information? Would you say it is very valuable, somewhat valuable, not very valuable, or not at all valuable? Percentage of 'very valuable' plus 'somewhat valuable' is shown. Margin of error is +/- 2.1% for blended online/phone respondents. Lighter green shading indicates a significantly higher score at a 95% confidence level versus other scores in the row.

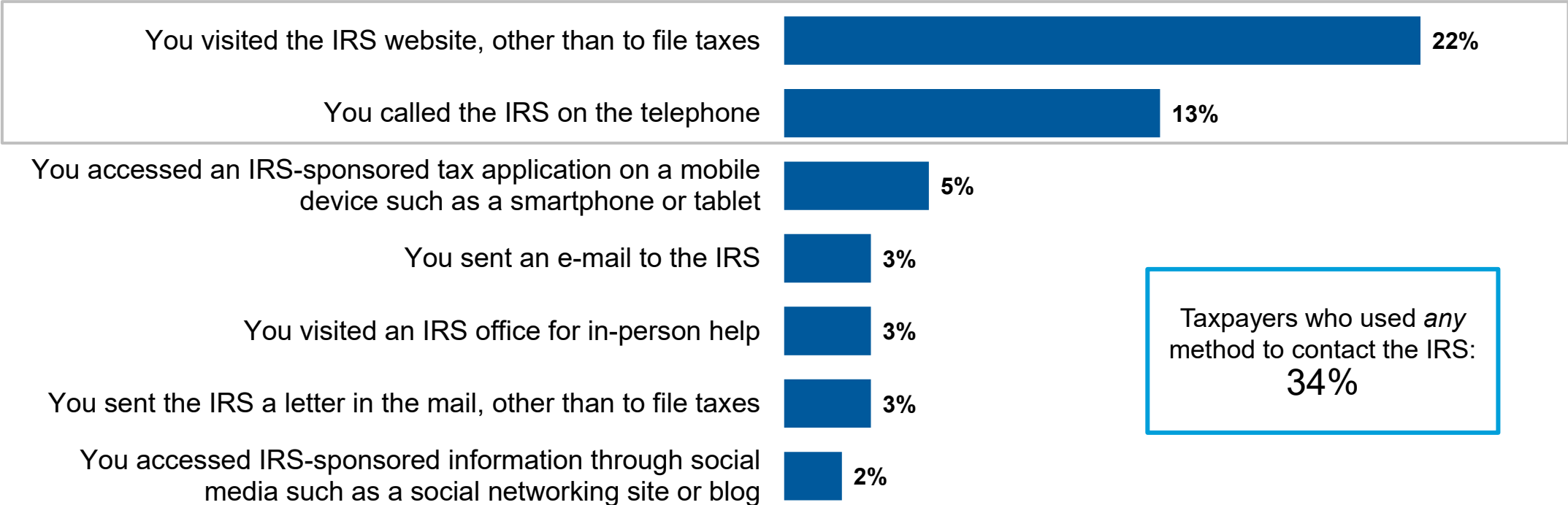
Taxpayers' perceived value from IRS printed publications for providing tax advice significantly decreased in 2020



Q9: How valuable would you say each of these sources is for getting tax advice or information? Would you say it is very valuable, somewhat valuable, not very valuable, or not at all valuable? Percentage of 'very valuable' plus 'somewhat valuable' is shown.
Margin of error is +/- 2.1% for blended online/phone respondents and +/- 3.1% for phone respondents only. Arrows indicate a statistical difference between 2019 and 2020 at a 95% confidence level.

In 2020, over a third of taxpayers contacted the IRS; most used the IRS website or the telephone

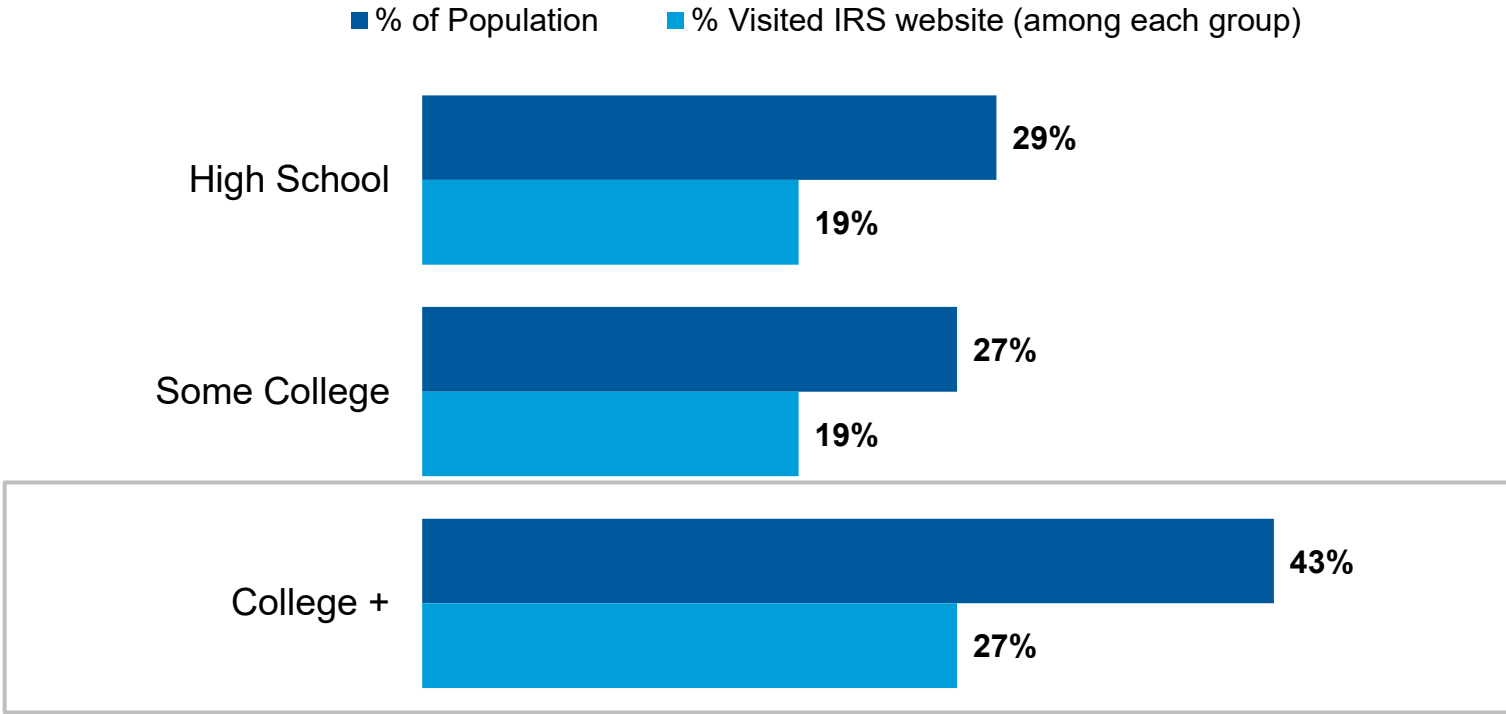
Method of contacting the IRS over the Past Year
(excluding filing of a tax return)



Q15: Thinking back over the past year, and excluding the filing of a tax return, did you initiate a contact with the IRS using any of the following methods?
Margin of error is +/- 2.1% for blended online/phone respondents.

Taxpayers with a college degree are significantly more likely to leverage the website to contact the IRS versus those with less education

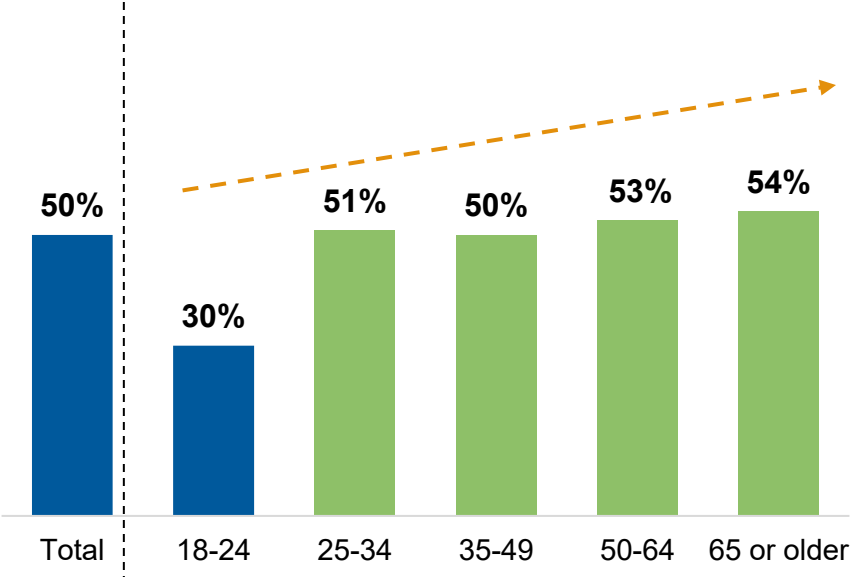
% Visited the IRS website, other than to file taxes, by Education



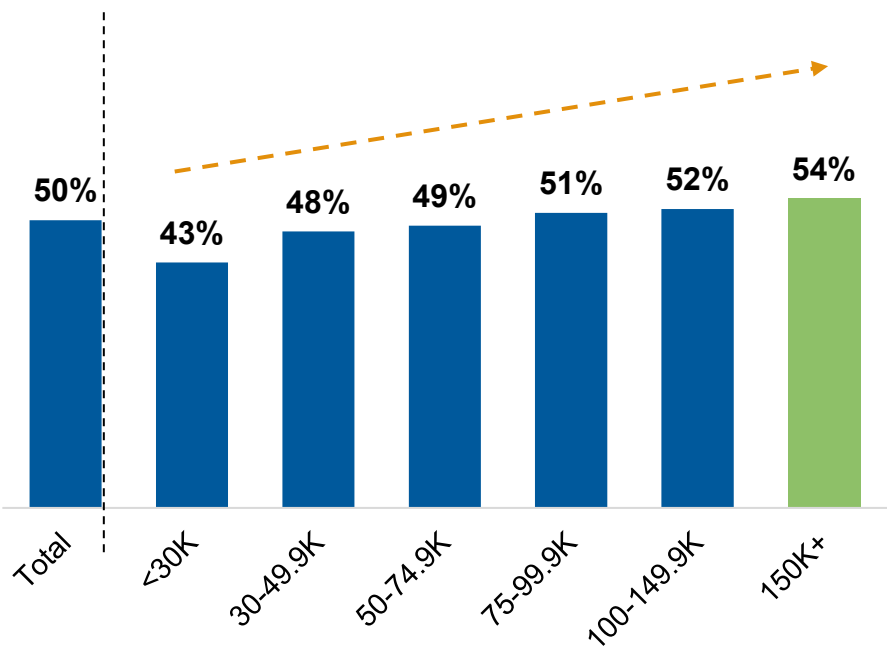
Q15: Thinking back over the past year, and excluding the filing of a tax return, did you initiate a contact with the IRS using any of the following methods?
Margin of error is +/- 2.1% for blended online/phone respondents. Green shading indicates a significantly higher score at a 95% confidence level versus other scores in the chart.

Half of taxpayers use a professional tax preparer; use of a paid tax preparer increases with age and income

Use of a Paid Tax Return Preparer for Most Recent Federal Income Tax Return by Age



Use of a Paid Tax Return Preparer for Most Recent Federal Income Tax Return by Income

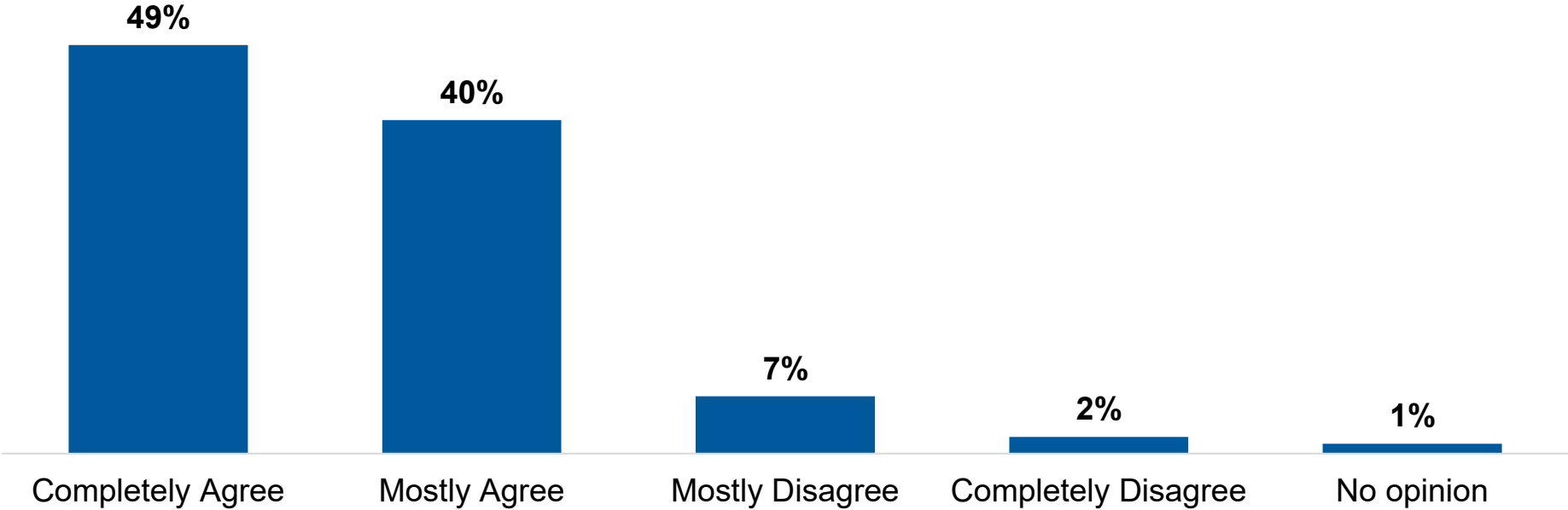


Q14: Did you use a paid tax return preparer to prepare your most recent Federal income tax return?
Margin of error is +/- 2.1% for blended online/phone respondents. Lighter green shading indicates a significantly higher score at a 95% confidence level versus other scores in the row.

IRS Services Provided to Taxpayers

Taxpayers agree more guidance from the IRS helps people correctly file their tax returns

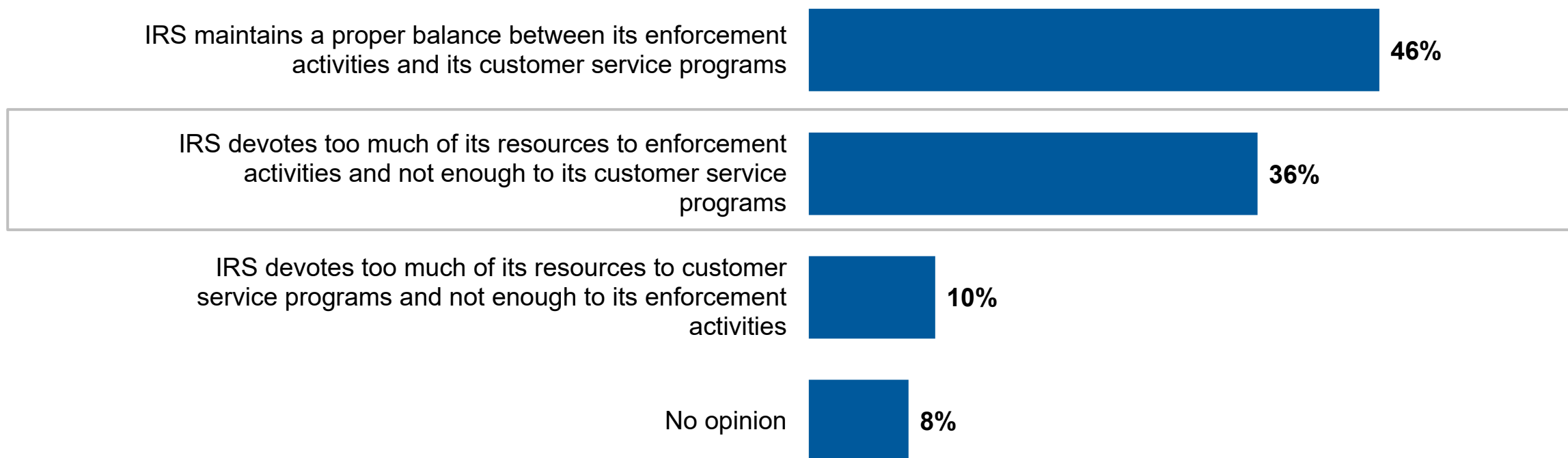
Agreement with ‘The more information and guidance the IRS provides, the more likely people are to correctly file their tax returns’



Q2: For each of the following statements, please indicate whether you completely agree, mostly agree, mostly disagree, or completely disagree.
Margin of error is +/- 2.1% for blended online/phone respondents.

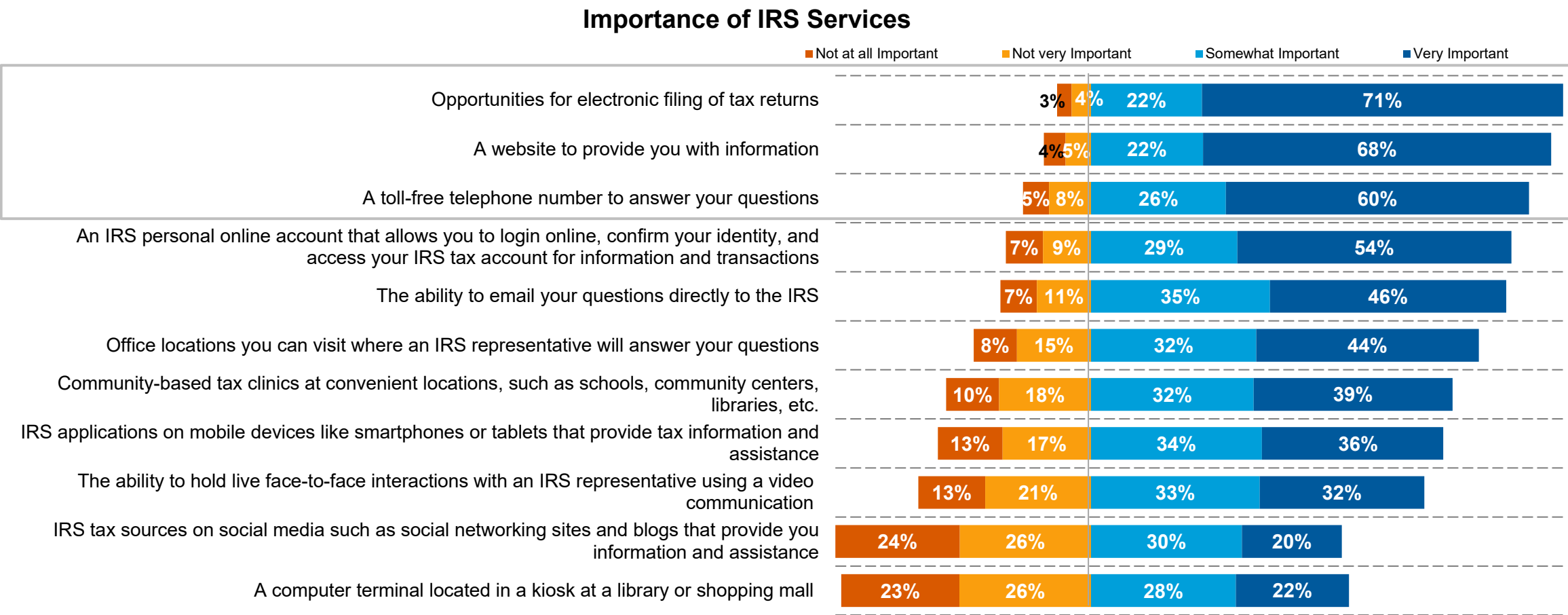
More than a third of taxpayers (36%) feel that the IRS devotes too much of its resources for enforcement and not as much for customer service

Statement Most Agreed With About the Resources the IRS Receives



Q10a: Considering the resources the IRS receives to do its job, which of the following statements do you most agree with? Do you feel that the...
Margin of error is +/- 2.1% for blended online/phone respondents.

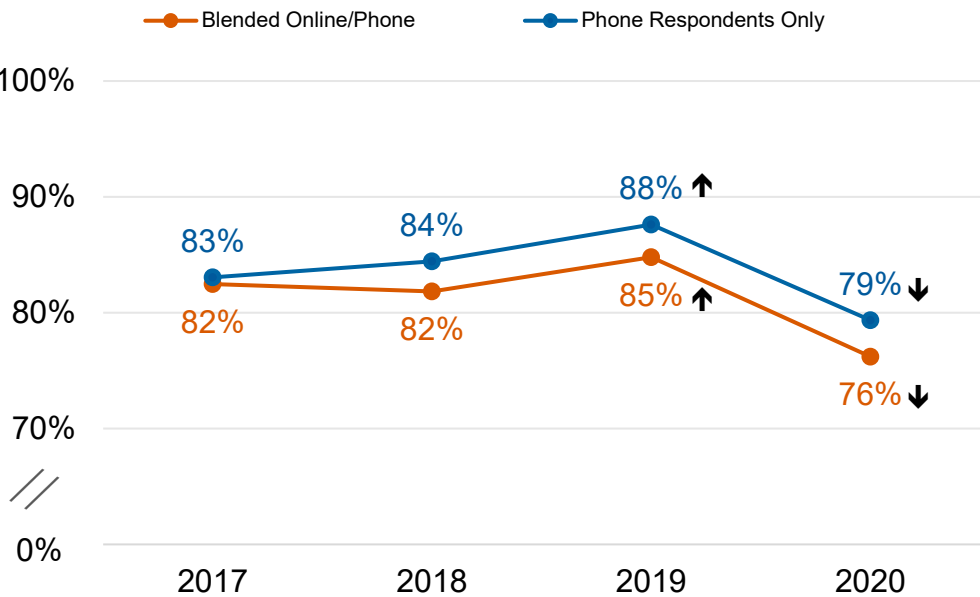
Taxpayers feel it's most important that the IRS provides opportunities to file taxes electronically, information on their website, and a toll-free number to answer questions



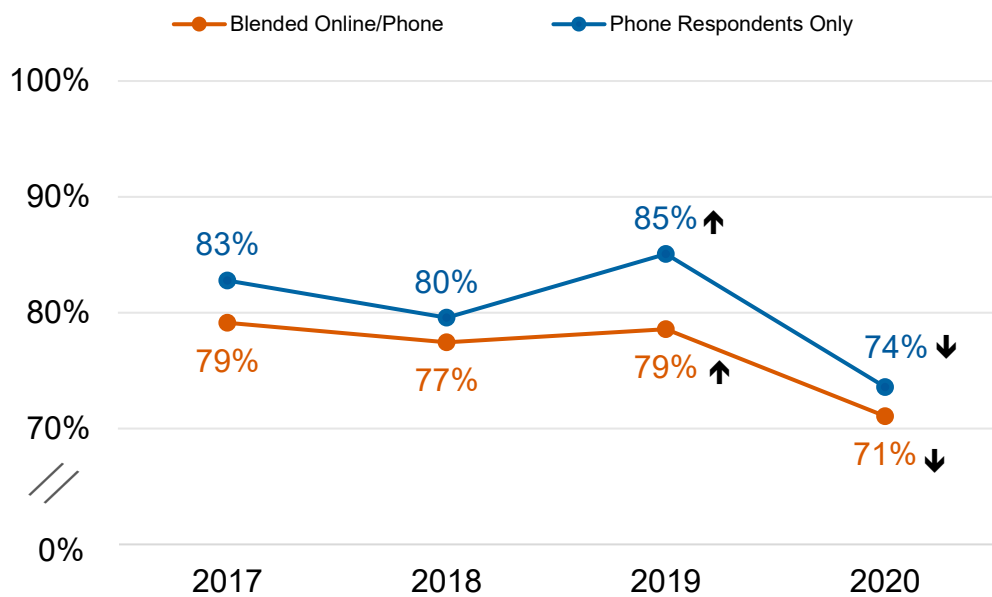
Q5: How important is it to you, as a taxpayer, that the IRS provides each of the following services to assist taxpayers?
Margin of error is +/- 2.1% for blended online/phone respondents. Note: Each stacked bar may not add up to 100% due to “don’t know,” “not applicable,” or “no response.”

The importance of each of the in-person IRS services significantly decreased in 2020 versus previous years

% Important : ‘IRS provides office locations you can visit where an IRS representative will answer your questions’



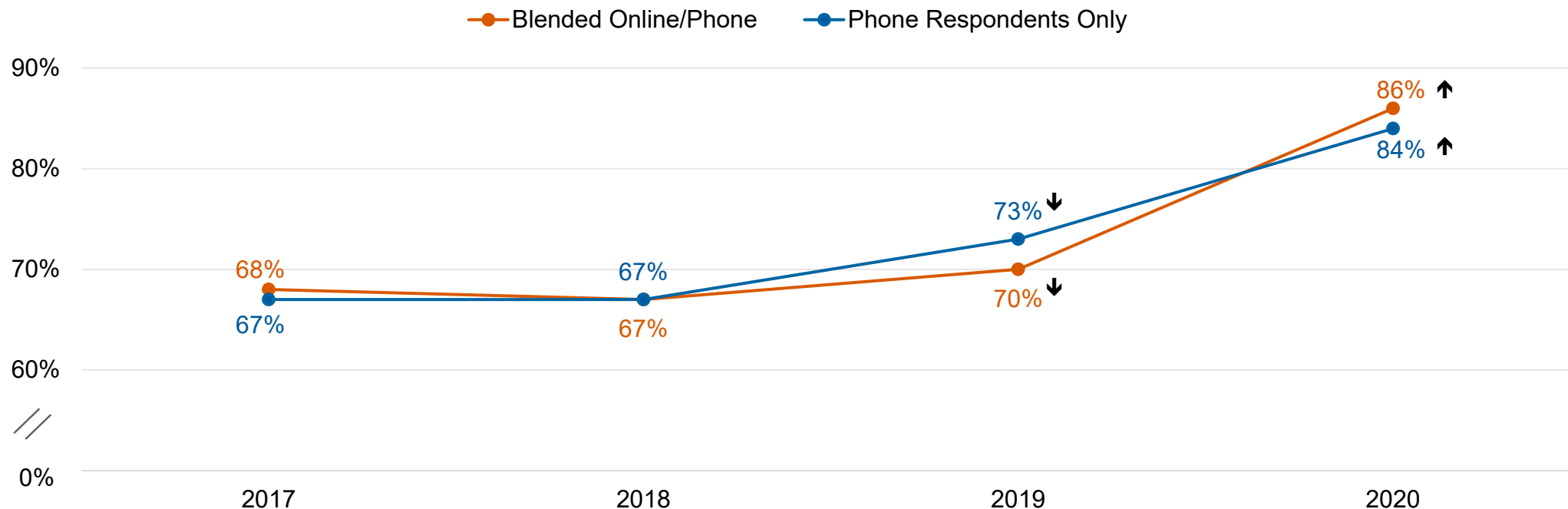
% Important: ‘Community-based tax clinics at convenient locations, such as schools, community centers, libraries, etc.’



Q5: How important is it to you, as a taxpayer, that the IRS provides each of the following services to assist taxpayers?
Margin of error is +/- 2.1% for blended online/phone respondents and +/- 3.1% for phone respondents only, Percentage ‘somewhat important’ plus ‘very important’ is shown. Arrows indicate a statistical difference between 2019 and 2020 at a 95% confidence level.

Yet, the share of taxpayers who agree the IRS should focus on improving in-person and phone call assistance to taxpayers continues to increase

Trend in % Agreeing 'The IRS should focus its efforts on improving in-person and phone call assistance to taxpayers'



Q11: For each of the following statements, please indicate whether you completely agree, mostly agree, mostly disagree, or completely disagree. Percentage 'completely agree' plus 'mostly agree' is shown.

Margin of error is +/- 2.1% for blended online/phone respondents and +/- 3.1% for phone respondents only. Arrows indicate a statistical difference between 2019 and 2020 at a 95% confidence level.

Notice 2014-21

SECTION 1. PURPOSE

This notice describes how existing general tax principles apply to transactions using virtual currency. The notice provides this guidance in the form of answers to frequently asked questions.

SECTION 2. BACKGROUND

The Internal Revenue Service (IRS) is aware that “virtual currency” may be used to pay for goods or services, or held for investment. Virtual currency is a digital representation of value that functions as a medium of exchange, a unit of account, and/or a store of value. In some environments, it operates like “real” currency -- i.e., the coin and paper money of the United States or of any other country that is designated as legal tender, circulates, and is customarily used and accepted as a medium of exchange in the country of issuance -- but it does not have legal tender status in any jurisdiction.

Virtual currency that has an equivalent value in real currency, or that acts as a substitute for real currency, is referred to as “convertible” virtual currency. Bitcoin is one example of a convertible virtual currency. Bitcoin can be digitally traded between users and can be purchased for, or exchanged into, U.S. dollars, Euros, and other real or virtual currencies. For a more comprehensive description of convertible virtual currencies to date, see Financial Crimes Enforcement Network (FinCEN) *Guidance on the Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies* (FIN-2013-G001, March 18, 2013).

SECTION 3. SCOPE

In general, the sale or exchange of convertible virtual currency, or the use of convertible virtual currency to pay for goods or services in a real-world economy transaction, has tax consequences that may result in a tax liability. This notice addresses only the U.S. federal tax consequences of transactions in, or transactions that use, convertible virtual currency, and the term “virtual currency” as used in Section 4 refers only to convertible virtual currency. No inference should be drawn with respect to virtual currencies not described in this notice.

The Treasury Department and the IRS recognize that there may be other questions regarding the tax consequences of virtual currency not addressed in this notice that warrant consideration. Therefore, the Treasury Department and the IRS request comments from the public regarding other types or aspects of virtual currency transactions that should be addressed in future guidance.

Comments should be addressed to:

Internal Revenue Service
Attn: CC:PA:LPD:PR (Notice 2014-21)
Room 5203
P.O. Box 7604
Ben Franklin Station
Washington, D.C. 20044

or hand delivered Monday through Friday between the hours of 8 A.M. and 4 P.M. to:

Courier's Desk
Internal Revenue Service
Attn: CC:PA:LPD:PR (Notice 2014-21)
1111 Constitution Avenue, N.W.
Washington, D.C. 20224

Alternatively, taxpayers may submit comments electronically via e-mail to the following address: Notice.Comments@irsounsel.treas.gov. Taxpayers should include "Notice 2014-21" in the subject line. All comments submitted by the public will be available for public inspection and copying in their entirety.

For purposes of the FAQs in this notice, the taxpayer's functional currency is assumed to be the U.S. dollar, the taxpayer is assumed to use the cash receipts and disbursements method of accounting and the taxpayer is assumed not to be under common control with any other party to a transaction.

SECTION 4. FREQUENTLY ASKED QUESTIONS

Q-1: How is virtual currency treated for federal tax purposes?

A-1: For federal tax purposes, virtual currency is treated as property. General tax principles applicable to property transactions apply to transactions using virtual currency.

Q-2: Is virtual currency treated as currency for purposes of determining whether a transaction results in foreign currency gain or loss under U.S. federal tax laws?

A-2: No. Under currently applicable law, virtual currency is not treated as currency that could generate foreign currency gain or loss for U.S. federal tax purposes.

Q-3: Must a taxpayer who receives virtual currency as payment for goods or services include in computing gross income the fair market value of the virtual currency?

A-3: Yes. A taxpayer who receives virtual currency as payment for goods or services must, in computing gross income, include the fair market value of the virtual currency,

measured in U.S. dollars, as of the date that the virtual currency was received. See Publication 525, *Taxable and Nontaxable Income*, for more information on miscellaneous income from exchanges involving property or services.

Q-4: What is the basis of virtual currency received as payment for goods or services in Q&A-3?

A-4: The basis of virtual currency that a taxpayer receives as payment for goods or services in Q&A-3 is the fair market value of the virtual currency in U.S. dollars as of the date of receipt. See Publication 551, *Basis of Assets*, for more information on the computation of basis when property is received for goods or services.

Q-5: How is the fair market value of virtual currency determined?

A-5: For U.S. tax purposes, transactions using virtual currency must be reported in U.S. dollars. Therefore, taxpayers will be required to determine the fair market value of virtual currency in U.S. dollars as of the date of payment or receipt. If a virtual currency is listed on an exchange and the exchange rate is established by market supply and demand, the fair market value of the virtual currency is determined by converting the virtual currency into U.S. dollars (or into another real currency which in turn can be converted into U.S. dollars) at the exchange rate, in a reasonable manner that is consistently applied.

Q-6: Does a taxpayer have gain or loss upon an exchange of virtual currency for other property?

A-6: Yes. If the fair market value of property received in exchange for virtual currency exceeds the taxpayer's adjusted basis of the virtual currency, the taxpayer has taxable gain. The taxpayer has a loss if the fair market value of the property received is less than the adjusted basis of the virtual currency. See Publication 544, *Sales and Other Dispositions of Assets*, for information about the tax treatment of sales and exchanges, such as whether a loss is deductible.

Q-7: What type of gain or loss does a taxpayer realize on the sale or exchange of virtual currency?

A-7: The character of the gain or loss generally depends on whether the virtual currency is a capital asset in the hands of the taxpayer. A taxpayer generally realizes capital gain or loss on the sale or exchange of virtual currency that is a capital asset in the hands of the taxpayer. For example, stocks, bonds, and other investment property are generally capital assets. A taxpayer generally realizes ordinary gain or loss on the sale or exchange of virtual currency that is not a capital asset in the hands of the taxpayer. Inventory and other property held mainly for sale to customers in a trade or

business are examples of property that is not a capital asset. See Publication 544 for more information about capital assets and the character of gain or loss.

Q-8: Does a taxpayer who “mines” virtual currency (for example, uses computer resources to validate Bitcoin transactions and maintain the public Bitcoin transaction ledger) realize gross income upon receipt of the virtual currency resulting from those activities?

A-8: Yes, when a taxpayer successfully “mines” virtual currency, the fair market value of the virtual currency as of the date of receipt is includible in gross income. See Publication 525, *Taxable and Nontaxable Income*, for more information on taxable income.

Q-9: Is an individual who “mines” virtual currency as a trade or business subject to self-employment tax on the income derived from those activities?

A-9: If a taxpayer’s “mining” of virtual currency constitutes a trade or business, and the “mining” activity is not undertaken by the taxpayer as an employee, the net earnings from self-employment (generally, gross income derived from carrying on a trade or business less allowable deductions) resulting from those activities constitute self-employment income and are subject to the self-employment tax. See Chapter 10 of Publication 334, *Tax Guide for Small Business*, for more information on self-employment tax and Publication 535, *Business Expenses*, for more information on determining whether expenses are from a business activity carried on to make a profit.

Q-10: Does virtual currency received by an independent contractor for performing services constitute self-employment income?

A-10: Yes. Generally, self-employment income includes all gross income derived by an individual from any trade or business carried on by the individual as other than an employee. Consequently, the fair market value of virtual currency received for services performed as an independent contractor, measured in U.S. dollars as of the date of receipt, constitutes self-employment income and is subject to the self-employment tax. See FS-2007-18, April 2007, *Business or Hobby? Answer Has Implications for Deductions*, for information on determining whether an activity is a business or a hobby.

Q-11: Does virtual currency paid by an employer as remuneration for services constitute wages for employment tax purposes?

A-11: Yes. Generally, the medium in which remuneration for services is paid is immaterial to the determination of whether the remuneration constitutes wages for employment tax purposes. Consequently, the fair market value of virtual currency paid as wages is subject to federal income tax withholding, Federal Insurance Contributions

Act (FICA) tax, and Federal Unemployment Tax Act (FUTA) tax and must be reported on Form W-2, *Wage and Tax Statement*. See Publication 15 (Circular E), *Employer's Tax Guide*, for information on the withholding, depositing, reporting, and paying of employment taxes.

Q-12: Is a payment made using virtual currency subject to information reporting?

A-12: A payment made using virtual currency is subject to information reporting to the same extent as any other payment made in property. For example, a person who in the course of a trade or business makes a payment of fixed and determinable income using virtual currency with a value of \$600 or more to a U.S. non-exempt recipient in a taxable year is required to report the payment to the IRS and to the payee. Examples of payments of fixed and determinable income include rent, salaries, wages, premiums, annuities, and compensation.

Q-13: Is a person who in the course of a trade or business makes a payment using virtual currency worth \$600 or more to an independent contractor for performing services required to file an information return with the IRS?

A-13: Generally, a person who in the course of a trade or business makes a payment of \$600 or more in a taxable year to an independent contractor for the performance of services is required to report that payment to the IRS and to the payee on Form 1099-MISC, *Miscellaneous Income*. Payments of virtual currency required to be reported on Form 1099-MISC should be reported using the fair market value of the virtual currency in U.S. dollars as of the date of payment. The payment recipient may have income even if the recipient does not receive a Form 1099-MISC. See the Instructions to Form 1099-MISC and the General Instructions for Certain Information Returns for more information. For payments to non-U.S. persons, see Publication 515, *Withholding of Tax on Nonresident Aliens and Foreign Entities*.

Q-14: Are payments made using virtual currency subject to backup withholding?

A-14: Payments made using virtual currency are subject to backup withholding to the same extent as other payments made in property. Therefore, payors making reportable payments using virtual currency must solicit a taxpayer identification number (TIN) from the payee. The payor must backup withhold from the payment if a TIN is not obtained prior to payment or if the payor receives notification from the IRS that backup withholding is required. See Publication 1281, *Backup Withholding for Missing and Incorrect Name/TINs*, for more information.

Q-15: Are there IRS information reporting requirements for a person who settles payments made in virtual currency on behalf of merchants that accept virtual currency from their customers?

A-15: Yes, if certain requirements are met. In general, a third party that contracts with a substantial number of unrelated merchants to settle payments between the merchants and their customers is a third party settlement organization (TPSO). A TPSO is required to report payments made to a merchant on a Form 1099-K, *Payment Card and Third Party Network Transactions*, if, for the calendar year, both (1) the number of transactions settled for the merchant exceeds 200, and (2) the gross amount of payments made to the merchant exceeds \$20,000. When completing Boxes 1, 3, and 5a-1 on the Form 1099-K, transactions where the TPSO settles payments made with virtual currency are aggregated with transactions where the TPSO settles payments made with real currency to determine the total amounts to be reported in those boxes. When determining whether the transactions are reportable, the value of the virtual currency is the fair market value of the virtual currency in U.S. dollars on the date of payment.

See The Third Party Information Reporting Center, <http://www.irs.gov/Tax-Professionals/Third-Party-Reporting-Information-Center>, for more information on reporting transactions on Form 1099-K.

Q-16: Will taxpayers be subject to penalties for having treated a virtual currency transaction in a manner that is inconsistent with this notice prior to March 25, 2014?

A-16: Taxpayers may be subject to penalties for failure to comply with tax laws. For example, underpayments attributable to virtual currency transactions may be subject to penalties, such as accuracy-related penalties under section 6662. In addition, failure to timely or correctly report virtual currency transactions when required to do so may be subject to information reporting penalties under section 6721 and 6722. However, penalty relief may be available to taxpayers and persons required to file an information return who are able to establish that the underpayment or failure to properly file information returns is due to reasonable cause.

SECTION 5. DRAFTING INFORMATION

The principal author of this notice is Keith A. Aqui of the Office of Associate Chief Counsel (Income Tax & Accounting). For further information about income tax issues addressed in this notice, please contact Mr. Aqui at (202) 317-4718; for further information about employment tax issues addressed in this notice, please contact Mr. Neil D. Shepherd at (202) 317- 4774; for further information about information reporting issues addressed in this notice, please contact Ms. Adrienne E. Griffin at (202) 317- 6845; and for further information regarding foreign currency issues addressed in this notice, please contact Mr. Raymond J. Stahl at (202) 317- 6938. These are not toll-free calls.

IRS Waves White Flag in Lawsuit Over Taxability of Cryptocurrency Staking Rewards

Taxpayer lawsuit demands confirmation of tax treatment of staking rewards

February 3, 2022 – Today, the Proof of Stake Alliance (POSA), a leading blockchain industry association, celebrated important news: as part of ongoing federal litigation (*Jarrett v. United States*, No. 3:21-cv-00419 (M.D. Tenn.)), the government has offered to refund plaintiff Joshua Jarrett for the taxes he paid when he created new property through staking, a sign that the IRS may no longer attempt to tax tokens created through staking moving forward. Despite this initial victory, Jarrett is refusing the refund and continuing with his case, as without such a ruling there will be nothing to prevent the IRS from challenging him again on this issue.

Jarrett paid income tax for 2019 on new tokens he created through staking. Contending that property that is created—like bread baked by a baker or a novel written by an author—is only taxed when it is sold, Jarrett filed for a refund in August 2020. The IRS ignored Jarrett’s refund claim, forcing him to pursue the matter in federal court. Today, court filings reveal that the government has offered to grant this refund, an early sign suggesting that the IRS will not tax property created through staking until it is sold.

POSA, and the broad coalition it represents, applauds Jarrett’s decision to continue his lawsuit. He has rejected the IRS’s offer of a refund, opening up the possibility of a court ruling that will give him, and millions of other taxpayers in the same position, the ability to confidently plan for the future. The importance of this issue has been raised by many, including Coin Center, the Blockchain Association, and several Members of Congress.

Proof of stake has skyrocketed in popularity as a blockchain consensus mechanism, with the market capitalization of the top 30 proof of stake tokens [approaching \\$600 billion](#) at the end of Q3 2021. Ethereum, which alone has a market cap of over \$260 billion, is [fully transitioning to proof of stake](#) later this year. Other popular blockchains including Solana, Cosmos, Avalanche, Cardano, and Tezos have long utilized the more environmentally friendly consensus method. In recent years, many of the largest US-based crypto-exchanges, including [Coinbase, Gemini, and Kraken](#), have started offering staking services to their retail customers, allowing millions of Americans to participate in securing blockchains and earning staking rewards—all of whom have the potential to run up against the same ambiguity with the IRS that Jarrett did. There is also a growing industry, including the two largest staking providers and US-based companies, [Bison Trails](#) (acquired by Coinbase) and [Blockdaemon](#) (now valued at over \$3.25B), that are focused on serving the staking ecosystem that would benefit from clear guidance from the IRS.

Abraham Sutherland, one of Jarrett’s lawyers, said, “While I appreciate the IRS’s offer, Jarrett needs a definitive ruling that the property he created through staking is not income.”

Evan Weiss, Founder of POSA added, "Proof of stake tokens will only increase in popularity in the coming years as web3 becomes mainstream, and the IRS must signal that it's prepared for innovations in the space. Back in 2019, we briefed officials at the Treasury Department as well as other policy makers on Capitol Hill about the need for a clear statement that staking rewards are not taxable income. Today we continue to urge the department to put forth an advisory that makes it clear that staking rewards will only be taxed when sold. We cannot risk making the US a second-rate market for staking, pushing the burgeoning multi-billion dollar staking industry to inevitably take those dollars elsewhere."

"The IRS doesn't just lay down in court, especially in cases that could affect millions of taxpayers on a very basic point of law. It means they've got a losing argument. For the sake of fair tax administration, and American innovation, I hope the IRS follows this up quickly with clear guidance that staking rewards aren't taxable income. As more and more blockchains use Proof of Stake to come to consensus and more and more American taxpayers participate in these networks, the government needs to catch up and apply years of settled tax law to the new property created by using this new technology," said Alison Mangiero, Board Member and acting Executive Director of POSA.

As Jarrett's legal battle continues, POSA hopes the IRS will affirm the existing legal status of staking rewards so that American taxpayers are not overtaxed or deterred from participating in this new technology.

Source: Proof of Stake Alliance
Dateline City: New York, NY

A Duty to Answer: Six Basic Questions and Recommendations for the IRS on Crypto Taxes

James T. Foust
April 2019

Coin Center Report



coincenter.org

James T. Foust, *A Duty to Answer: Six Basic Questions and Recommendations for the IRS on Crypto Taxes*, Coin Center Report, April 2019, available at <https://coincenter.org/entry/crypto-tax-questions>

Abstract

U.S. taxpayers lack answers to basic questions about the federal tax and reporting effects of transactions involving cryptocurrencies. Although the Internal Revenue Service has been examining issues related to the taxation of “virtual property” and “virtual currencies” for over a decade, it has only issued one piece of guidance about them. That guidance, published in early 2014 and applicable only to “convertible” virtual currency, fails to answer basic questions like:

1. How should taxpayers distinguish between convertible and non-convertible virtual currency, and what is the significance of that distinction?
2. How should taxpayers determine the fair market value of their cryptocurrency?
3. How should taxpayers calculate the basis of cryptocurrency dispositions?
4. How should taxpayers substantiate the value of cryptocurrency donations?
5. How should taxpayers account for tokens they receive from a network fork or airdrop?
6. How should taxpayers account for cryptocurrency when filing information returns?

Numerous stakeholders within and without the government have noted the 2014 guidance’s failure to address these and other basic tax questions, and have made repeated requests to the IRS for additional clarity. This report adds to that body of exhortation and recommends actions the IRS could take to resolve these open questions. Rather than indicating any intention to provide additional guidance, the IRS seems to be ramping up enforcement activities against taxpayers who “misreport” the tax consequences of their cryptocurrency transactions.

Author

James T. Foust
Coin Center
james@coincenter.org

About Coin Center

Coin Center is a non-profit research and advocacy center focused on the public policy issues facing open blockchain technologies such as Bitcoin. Our mission is to build a better understanding of these technologies and to promote a regulatory climate that preserves the freedom to innovate using blockchain technologies. We do this by producing and publishing policy research from respected academics and experts, educating policymakers and the media about blockchain technology, and by engaging in advocacy for sound public policy.

Acknowledgements

Thank you to my Coin Center colleagues Neeraj Agrawal, Jerry Brito, Peter Van Valkenburgh, and Robin Weisman for indispensable help on early drafts of this paper, and to Andrea Castillo for invaluable research assistance. Sincere thanks to those who provided comments on this paper. Any and all mistakes are solely my own.

The advent of cryptocurrencies has given rise to many interesting, and often complex, policy questions about how existing regulatory regimes ought to be applied to, or adapted to, this new and disruptive technology. Federal agencies have made significant progress in addressing some of these questions, such as when digital assets are securities for purposes of U.S. securities law and what types of activities qualify a cryptocurrency user as a Money Service Business in the eyes of the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN). In other areas there has been disappointingly little progress in spite of repeated requests for clarity from within and without the government. One such area is the federal tax treatment of cryptocurrencies.

Housed within the U.S. Department of the Treasury, the Internal Revenue Service (IRS) is tasked with "help[ing] the large majority of compliant taxpayers with the tax law, while ensuring that the minority who are unwilling to comply pay their fair share."¹ Operating under authority of the Internal Revenue Code of 1986 (IRC), the IRS administers and supervises the execution and application of federal tax law.

The IRS has been aware of the tax ambiguities of virtual currencies, and the concomitant need for clear guidance, for over a decade. In 2008, the agency's Taxpayer Advocate Service identified "emerging issues such as those arising from 'virtual worlds'" as one of "the most serious problems encountered by taxpayers" in its annual report to Congress.² Although blockchain-based cryptocurrencies like Bitcoin did not yet exist, the growth of significant economic activity within video games such as World of Warcraft and Second Life prompted the Taxpayer Advocate to recommend that the IRS provide clear guidance on many of the tax ambiguities that still plague cryptocurrency users today, such as:

[I]s a person subject to tax each time he or she acquires virtual property? How about when the person exchanges one virtual property for another, or for virtual currency? How about when the user sells the virtual property or his or her account (and avatar) for real money? What, if any, information reporting, withholding, backup withholding, and recordkeeping requirements apply to these transactions?³

The Taxpayer Advocate ends with a piece of advice that is particularly relevant today, and which we hope the IRS will heed:

As the tax administrator, the IRS has a duty to answer all of the basic questions about transactions undertaken regularly by significant numbers of taxpayers, such as those involving virtual items (described above), especially if the questions are difficult for taxpayers to answer on their own. It may be unfair to expect the IRS to answer these questions before state property and contract

¹ Internal Revenue Service, "The Agency, its Mission, and Statutory Authority," *IRS website* (Feb. 6, 2019) <https://www.irs.gov/about-irs/the-agency-its-mission-and-statutory-authority>.

² Internal Revenue Service, "National Taxpayer Advocate: 2008 Annual Report to Congress (Volume 1)," *IRS Publication 2104 (Rev. 12-2008)* (Dec. 31, 2008) p.216, https://www.irs.gov/pub/tas/08_tas_arc_intro_toc_msp.pdf.

³ *Id.* at p.218.

laws have evolved far enough to provide clear guidance about when a transfer of virtual items is a transfer of property rights. These very difficulties, however, support the conclusion that the IRS should issue guidance. If the tax experts at the IRS cannot figure out what the rules are or should be, unsophisticated taxpayers who participate in the virtual economy have little hope of doing so. The IRS could at least make an administrative pronouncement about how taxpayers should treat these transactions in the interim as it studies the issue and the state law rules evolve.

More broadly, the IRS needs to produce specific early guidance on difficult issues confronted by taxpayers on a regular basis in emerging areas of economic activity. Otherwise, it risks turning these taxpayers into unintentional tax cheats, establishing noncompliance norms in the industry, and leaving IRS employees without clear guidance about how to do their jobs.⁴

In 2008, World of Warcraft had about 2.5 million subscribers in North America;⁵ Second Life is not subscription-based and does not routinely publish active user statistics, but is generally believed to have peaked at around 1 million monthly active users worldwide in 2013.⁶ A recent survey of U.S. consumers by the Federal Reserve Bank of New York's Center for Microeconomic Data found that "[a]round 5 percent of respondents reported that they currently or previously owned cryptocurrency and an additional 15 percent reported that they were considering buying cryptocurrency."⁷ Taking into account that there are roughly 250 million adults living in the United States,⁸ cryptocurrency users likely constitute a larger portion of the current population than Word of Warcraft and Second Life players did in 2008 when the Taxpayer Advocate indicated that they made up "significant numbers of taxpayers," and, as such, that the agency had "a duty to answer all of the basic questions about transactions undertaken regularly by [them.]"⁹

Following a 2013 report from the U.S. Government Accountability Office (GAO) recommending the IRS "find relatively low-cost ways to provide information to taxpayers . . . on the basic tax

⁴ *Id.* at p.225 (footnotes omitted).

⁵ Blizzard, "World of Warcraft Reaches New Milestone: 10 Million Subscribers," *Press Release* (Jan. 22, 2008) <http://eu.blizzard.com/en-gb/company/press%20/pressreleases.html?id=10014593>.

⁶ Samuel Axon, "Returning to Second Life," *Ars Technica* (Oct. 23, 2017) <https://arstechnica.com/gaming/2017/10/returning-to-second-life/>; Linden Lab, "Infographic: 10 Years of Second Life," *Press Release* (Jun. 20, 2013) <https://www.lindenlab.com/releases/infographic-10-years-of-second-life>.

⁷ Sean Hundtofte, Michael Lee, Antoine Martin, and Reed Orchinik, "Deciphering American's Views on Cryptocurrencies," *Liberty Street Economics, Federal Reserve Bank of New York* (Mar. 25, 2019) <https://libertystreeteconomics.newyorkfed.org/2019/03/deciphering-americans-views-on-cryptocurrencies.html>.

⁸ U.S. Census Bureau, "2005-2009 American Community Survey 5-Year Estimates," *American FactFinder Database* (accessed Apr. 2, 2019) available at https://factfinder.census.gov/bkmk/table/1.0/en/ACS/17_5YR/S0101.

⁹ Internal Revenue Service, "National Taxpayer Advocate: 2008 Annual Report to Congress (Volume 1)," *IRS Publication 2104 (Rev. 12-2008)* (Dec. 31, 2008) p.225, https://www.irs.gov/pub/tas/08_tas_arc_intro_toc_msp.pdf.

reporting requirements for transactions using virtual currencies,”¹⁰ the IRS issued Notice 2014-21, *Virtual Currency Guidance*, in early 2014.¹¹ The IRS also established a Virtual Currency Issue Team in December 2013.¹²

Drawing from FinCEN’s 2013 virtual currency guidance,¹³ Notice 2014-21 defines “virtual currency” to be “a digital representation of value that functions as a medium of exchange, a unit of account, and/or a store of value . . . but it does not have legal tender status in any jurisdiction.”¹⁴ It further defines “convertible” virtual currency to be a virtual currency that “has an equivalent value in real currency, or that acts as a substitute for real currency” and identifies that “Bitcoin is one example[.]”¹⁵ It then specifies that the guidance only applies to convertible virtual currencies. The notice’s substantive guidance is a 16-question FAQ section providing certain basic information about the federal tax treatment of virtual currencies.

While some guidance is better than none, Notice 2014-21 fails to resolve many ambiguities related to virtual currency taxation. In 2016, the Treasury Inspector General for Tax Administration (TIGTA) found that:

Although the IRS issued Notice 2014-21, Virtual Currency Guidance, and established the Virtual Currency Issue Team, there has been little evidence of coordination between the responsible functions to identify and address, on a program level, potential taxpayer noncompliance issues for transactions

¹⁰ James R. White, et al., “Virtual Economies and Currencies, Additional IRS Guidance Could Reduce Tax Compliance Risks,” *Government Accountability Office Report to the Senate Committee on Finance (GAO-13-516)* (May 2013) <https://www.gao.gov/assets/660/654620.pdf>.

¹¹ Internal Revenue Service, “IRS Virtual Currency Guidance,” *IRS Notice 2014-21* (Apr. 14, 2014) <https://www.irs.gov/pub/irs-drop/n-14-21.pdf>.

¹² Treasury Inspector General for Tax Administration, “As the Use of Virtual Currencies in Taxable Transactions Becomes More Common, Additional Actions Are Needed to Ensure Taxpayer Compliance,” *TIGTA Report No. 2016-30-083* (Sep. 21, 2016) at p.3, <https://www.treasury.gov/tigta/auditreports/2016reports/201630083fr.pdf> (“According to IRS management, the Large Business and International Division’s Offshore Arrangements Practice Network Steering Committee established the Virtual Currency Issue Team (VCIT) in December 2013 to get a better understanding of how virtual currencies may affect international taxable transactions. Specifically, the original focus of the VCIT was the identification of international underreporting strategies using virtual currency to facilitate tax avoidance/evasion schemes. In April 2015, the VCIT’s focus was expanded to act as a forum for interested individuals from various IRS offices and functions to meet and share knowledge on virtual currency. The VCIT includes members from the IRS’s Office of Chief Counsel and Criminal Investigation as well as the Large Business and International Division and the Small Business/Self-Employed Division. The VCIT’s current efforts are to: 1) determine if virtual currencies are being used as a method to hide income and avoid U.S. taxation; 2) be a vehicle to share virtual currency knowledge across the IRS; and 3) identify audit techniques that can be used to determine if taxpayers using virtual currencies in transactions, especially in offshore arrangements, are attempting to conceal income and avoid U.S. taxation.”).

¹³ U.S. Department of the Treasury, Financial Crimes Enforcement Network, “Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies,” *Guidance FIN-2013-G001* (Mar. 18, 2013) <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf>.

¹⁴ Internal Revenue Service, “IRS Virtual Currency Guidance,” *IRS Notice 2014-21* (Apr. 14, 2014) <https://www.irs.gov/pub/irs-drop/n-14-21.pdf>.

¹⁵ *Id.*

involving virtual currencies. None of the IRS operating divisions have developed any type of compliance initiatives or guidelines for conducting examinations or investigations specific to tax noncompliance related to virtual currencies. . . . Although the IRS requested comments to Notice 2014-21 from the public, no actions were taken to address the comments received. TIGTA reviewed all the comments and found several examples of information requested by the public that would be helpful in understanding how to comply with the tax reporting requirements when using or receiving virtual currencies.¹⁶

In light of these findings, TIGTA recommended that the IRS “should take action to provide updated guidance to reflect the documentation requirements and tax treatments needed for the various uses of virtual currencies.”¹⁷ In a response, the IRS “agreed that additional guidance would be helpful,” but also “conveyed that guidance allocation decisions are based on available resources and other competing organizational and legislative priorities.”¹⁸ TIGTA noted that “the IRS’s current guidance related to virtual currencies is insufficient. To help taxpayers voluntarily comply with their tax obligations, the IRS should devote some of its efforts to provide adequate direction in this new and complex area.”¹⁹

The IRS has not released further guidance since Notice 2014-21, and the TIGTA report above notes “[d]uring discussions with IRS management, our auditors were told that no changes to the IRS guidance would be made based on the comments received from the public.”²⁰ The IRS has, however, signaled a more aggressive enforcement stance towards taxpayers that misreport their virtual-currency-related tax obligations. In late 2016, the Department of Justice, on behalf of the IRS, requested permission from the U.S. District Court for the Northern District of California to serve a “John Doe summons” on Coinbase, a large virtual currency exchange based in San Francisco, directing the exchange to produce records identifying all U.S. taxpayers who had used its services at any point in 2013, 2014, or 2015, as well as documentation of those taxpayers’ virtual currency transactions.²¹ Brian Armstrong, the CEO of Coinbase, noted at the time that the request would cover millions of consumer accounts and that “[a]sking for detailed transaction information on so many people, simply for using digital currency, is a violation of

¹⁶ Treasury Inspector General for Tax Administration, “As the Use of Virtual Currencies in Taxable Transactions Becomes More Common, Additional Actions Are Needed to Ensure Taxpayer Compliance,” *TIGTA Report No. 2016-30-083* (Sep. 21, 2016) at p.3 (“Highlights: What TIGTA found”), <https://www.treasury.gov/tigta/auditreports/2016reports/201630083fr.pdf>.

¹⁷ *Id.* at p.11.

¹⁸ *Id.* at p.11.

¹⁹ *Id.* at p.12.

²⁰ *Id.* at p.11.

²¹ The request was later narrowed significantly, to only include documentation of Coinbase customers that had transacted more than \$20,000 over the course of a year. See: Department of Justice, “Court Authorizes Service of John Doe Summons Seeking the Identities of U.S. Taxpayers Who Have Used Virtual Currency,” *DOJ Press Release No. 16-1404* (Nov. 30, 2016) <https://www.justice.gov/opa/pr/court-authorizes-service-john-doe-summons-seeking-identities-us-taxpayers-who-have-used>.

their privacy, and is not the best way for [Coinbase and the IRS] to accomplish our mutual objective [for all U.S. users of virtual currency to pay their taxes].”²²

In March 2018, the IRS published a news release, “IRS reminds taxpayers to report virtual currency transactions,” stating, in part:

Taxpayers who do not properly report the income tax consequences of virtual currency transactions can be audited for those transactions and, when appropriate, can be liable for penalties and interest.

In more extreme situations, taxpayers could be subject to criminal prosecution for failing to properly report the income tax consequences of virtual currency transactions. Criminal charges could include tax evasion and filing a false tax return. Anyone convicted of tax evasion is subject to a prison term of up to five years and a fine of up to \$250,000. Anyone convicted of filing a false return is subject to a prison term of up to three years and a fine of up to \$250,000.²³

And, on July 2, 2018, the IRS announced a compliance campaign focusing on virtual currencies that “will address noncompliance related to the use of virtual currency through multiple treatment streams including outreach and examinations . . . Taxpayers with unreported virtual currency transactions are urged to correct their returns as soon as practical.”²⁴

In its 2018 General Report, released in October, the IRS’s Information Reporting Program Advisory Committee (IRPAC) wrote, “[w]hile we acknowledge and thank the IRS for publishing Notice 2014-21 . . . many industry and tax practitioners still question other tax consequences of cryptocurrency transactions . . . Therefore, IRPAC recommends that the IRS issue further guidance on the tax consequences of cryptocurrency transactions.”²⁵ The IRS Advisory Council (IRSAC), which released its 2018 Annual Report in November, also highlighted the need for the agency to do a better job providing guidance on the taxation of virtual currencies. The group’s first recommendation on the matter states:

Consider the Proposals and Comments Received. Notice 2014-21 was issued four years ago. Considering the increased prevalence of virtual currency, Notice 2014-21 does not adequately address many tax issues arising from such transactions. In addition to the public comments, several tax-related

²² Brian Armstrong, “Coinbase and the IRS,” *Medium* (Jan. 14, 2017) <https://medium.com/@barmstrong/coinbase-and-the-irs-c4e2e386e0cf>.

²³ Internal Revenue Service, “IRS reminds taxpayers to report virtual currency transactions,” *IRS News Release IR-2018-71* (Mar. 23, 2018) <https://www.irs.gov/newsroom/irs-reminds-taxpayers-to-report-virtual-currency-transactions>.

²⁴ Internal Revenue Service, “IRS Announces the Identification and Selection of Five Large Business and International Compliance Campaigns,” *IRS News Release* (Jul. 2, 2018) <https://www.irs.gov/businesses/irs-announces-the-identification-and-selection-of-five-large-business-and-international-compliance-campaigns>.

²⁵ Dana Flynn, et al., “Information Reporting Advisory Committee Public Report,” *IRS Publication 5315*, Catalog Number 71819H (Oct. 2018) at p.8, <https://www.irs.gov/pub/irs-pdf/p5315.pdf>.

professional organizations proposed areas of guidance relating to virtual currency needed by taxpayers and tax professionals. The IRSAC has reviewed the recommendations for guidance submitted by the American Institute of CPAs (AICPA) and the American Bar Association (ABA) Taxation Section and strongly supports these recommendations. The IRSAC also recommends the IRS identify guidance relating to virtual currency on its upcoming 2018-2019 Priority Guidance Plan.²⁶

In the same month as that report was published, the IRS and Treasury Department jointly released the 2018-2019 Priority Guidance Plan, which identifies 239 guidance projects that will be the focus of the 12-month period from July 2018 through June 2019. Virtual currency guidance is not among the projects so identified.²⁷

In some ways, the IRS's reticence in providing clear virtual currency tax guidance is understandable. After all, the tax code and its implementing regulations are notoriously complex, some of the tax questions raised by virtual currencies are complicated and novel, and regulatory agencies generally are reluctant to make public statements that may later need to be modified or walked back in light of changes in the underlying facts and circumstances (and/or in light of changes in the agency's understanding of those facts and circumstances). However, until the IRS provides clarity on how taxpayers should account for virtual currency activity when filing their tax returns, it would be unjust for it to begin cracking down on them for failing to do so.

This paper describes what virtual currency tax questions Notice 2014-21 answered, identifies several pressing ambiguities that remain, and recommends solutions to those ambiguities. It is focused on individuals who participate in the cryptocurrency ecosystem in a personal capacity—it does not delve into state tax, corporate tax, or issues faced by brokers, dealers, and professional traders in securities and commodities, although there are certainly open questions in those areas as well.

Open Questions and Recommendations for Guidance

Notice 2014-21 states that “[f]or federal tax purposes, virtual currency is treated as property. General tax principles applicable to property transactions apply to transactions using virtual currency.”²⁸ While the notice addresses the general classification of convertible virtual currencies as property for federal income tax purposes, it fails to provide sufficient specificity for one to determine which particular “general tax principles” should be applied to them. This may have been reasonable at the time the notice was issued; however, federal income tax consequences will, with few exceptions, depend upon a more specific classification of virtual

²⁶ Dennis Ventry, Jr., et al., “Information Reporting Advisory Committee Public Report,” *IRS Publication 5316*, Catalog Number 71824A (Nov. 2018) at pp. 75-76, <https://www.irs.gov/pub/irs-pdf/p5316.pdf>.

²⁷ David Kautter, Charles P. Rettig, and William M. Paul, 2018-2019 Priority Guidance Plan,” Department of the Treasury Office of Tax Policy and Internal Revenue Service (Oct. 31, 2018) https://www.irs.gov/pub/irs-utl/2018-2019_pgp_initial.pdf.

²⁸ Internal Revenue Service, “IRS Virtual Currency Guidance,” *IRS Notice 2014-21* (Apr. 14, 2014) at p.2, <https://www.irs.gov/pub/irs-drop/n-14-21.pdf>. (Q-1: “How is virtual currency treated for tax purposes?”).

currency as being, for purposes of the particular section of the IRC and its implementing regulations at hand, money, commodity, security, a subcategory of one of the foregoing, or something else. The IRC (and implementing regulations) is an immense body of law; it contains many highly specific sections and subsections, each of which addresses a particular aspect of the particular taxation principles that apply to particular types of property and, in doing so, ascribes either explicitly or implicitly to its key terms the definitions which are most appropriate for its purposes. Frequently with high-level terms like “property,” “money,” “commodity,” or “security,” different sections of the IRC (and implementing regulations) provide conflicting definitions for a particular term (or provide definitions for subsets of a term which include items that fall outside other sections’ definitions of that term) while others use the term without indicating what definition is meant.²⁹ For guidance on cryptocurrency taxation to be meaningful, it must acknowledge this complexity and specifically classify how cryptocurrencies fit within it or, better yet, provide a framework for doing so. What follows are Coin Center’s recommendations for such guidance on several open questions about the taxation of cryptocurrency transactions.

Open Question 1: How should taxpayers distinguish between convertible and non-convertible virtual currency, and what is the significance of that distinction?

It is important to note that the guidance in Notice 2014-21 applies *only* to “convertible virtual currency.” According to the guidance,

Virtual currency is a digital representation of value that functions as a medium of exchange, a unit of account, and/or a store of value. In some environments, it operates like ‘real’ currency—i.e., the coin and paper money of the United States or of any other country that is designated as legal tender, circulates, and is customarily used and accepted as a medium of exchange in the country of issuance—but it does not have legal tender status in any jurisdiction.³⁰

A subset of virtual currency is “convertible” virtual currency, which the guidance states is “[v]irtual currency that has an equivalent value in real currency, or that acts as a substitute for real currency[.]”³¹ In Notice 2014-21, the IRS gives one example of a convertible virtual currency—Bitcoin—and stresses that “[n]o inference should be drawn [from this notice] with

²⁹ For example, 26 U.S.C. § 351(e)(1)(B) specifies that, for its purposes, the term “stock and securities” includes “money” and “foreign currencies,” and 26 U.S.C. § 6045(g)(3)(B) states that, for its purposes, “specified security” includes “any commodity, or contract or derivative with respect to such commodity, if the Secretary determines that adjusted basis reporting is appropriate for purposes of this subsection[.]” 26 U.S.C. § 731(c)(1)(A), on the other hand, says that, for its purposes, the term “money” includes “securities,” contingent on several qualifications. Meanwhile 26 U.S.C. § 317 defines “property” as “money, securities, and any other property[.]” There is one section of the IRC, 26 U.S.C. § 614(a), titled “definition of property.” It begins: “For the purpose of computing the depletion allowance in the case of mines, wells, and other natural deposits, the term ‘property’ means means each separate interest owned by the taxpayer in each mineral deposit in each separate tract or parcel of land.”

³⁰ Internal Revenue Service, “IRS Virtual Currency Guidance,” *IRS Notice 2014-21* (Apr. 14, 2014) at p.1, <https://www.irs.gov/pub/irs-drop/n-14-21.pdf>.

³¹ *Ibid.*

respect to virtual currencies not described in this notice.”³² It seems likely this definition would include cryptocurrencies like Ethereum and Zcash, both of which did not yet exist at the time of Notice 2014-21 but which are broadly similar to Bitcoin. It is unclear, however, whether Notice 2014-21 applies to substantially different types of digital assets such as those having attached voting or payment rights or other contractual rights or obligations, algorithmic stablecoins, airline rewards miles, and video game currencies for which there are official fiat markets—e.g., Second Life’s Linden Dollars—as well as video game currencies that are not meant to be traded for fiat but for which secondary black markets nevertheless exist—e.g., World of Warcraft Gold.

As noted above, the IRS appears to have drawn from FinCEN’s 2013 guidance for Notice 2014-21’s definition of “virtual currency” generally and “convertible virtual currency” as a specific subset thereof.³³ FinCEN’s mandate is to “safeguard the financial system from illicit use, combat money laundering, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.”³⁴ Distinguishing between convertible and non-convertible virtual currencies makes sense in that context: FinCEN is concerned with the movement of funds through the financial system and will naturally take more interest in virtual currencies that can readily be converted to and from fiat—i.e., “convertible” virtual currencies—than it will in virtual currencies that are illiquid. In contrast, it is not readily apparent why such a distinction is important in the context of federal income taxes. To our knowledge, the IRS has not explained why it decided to bifurcate virtual currency tax guidance in this way, nor has it issued any guidance on the taxation of non-convertible virtual currencies.³⁵

³² *Ibid.*

³³ *Supra* note 13.

³⁴ Financial Crimes Enforcement Network, “Mission,” *FinCEN Website* (accessed Apr. 2, 2019) <https://www.fincen.gov/about/mission>.

³⁵ A number of other federal agencies have weighed in on virtual currency issues without restricting their statements’ applicability to only convertible virtual currency or to only non-convertible virtual currency. See, e.g., Consumer Financial Protection Bureau, “Risks to consumers posed by virtual currencies,” *CFPB Consumer Advisory* (Aug. 2014) https://files.consumerfinance.gov/f/201408_cfpb_consumer-advisory_virtual-currencies.pdf (describing “virtual currencies,” without reference to “convertibility,” as, in part, “a kind of electronic money” that “[isn’t] regular money,” and is “not issued or backed by the United States or any other government or central bank. No one is required to accept them as payment or to exchange them for traditional currencies. . . .”); Commodity Futures Trading Commission, “An Introduction to Virtual Currency,” https://www.cftc.gov/sites/default/files/idc/groups/public/%40customerprotection/documents/file/oceo_aivc0218.pdf (noting “[s]ome virtual currencies have an equivalent value in other currencies, such as U.S. dollars or Euros, or can be traded for other virtual currencies. These are referred to as convertible virtual currencies. Bitcoin is an example of a convertible virtual currency,” but not making further use of the distinction.); Commodity Futures Trading Commission, “CFTC Backgrounder on Oversight of and Approach to Virtual Currency Futures Markets” (Jan. 4, 2018) https://www.cftc.gov/sites/default/files/idc/groups/public/%40customerprotection/documents/file/backgrounder_virtualcurrency01.pdf (providing an overview of CFTC’s jurisdiction over, and approach to regulating, virtual currencies as commodities without making any distinction between convertible and non-convertible virtual currency.).

Separately, It is also unclear what the tax treatment of Bitcoin (or other convertible virtual currency) would be if a foreign nation passed a law making it legal tender, which could disqualify it from Notice 2014-21's requirement that, for the notice's purposes, virtual currency "not have legal tender status in any jurisdiction."³⁶

Beginning with the next section and continuing through the rest of this report, we will use the term "virtual currency" in the same sense that the IRS uses it in Notice 2014-21: "virtual currency" means "convertible virtual currency," which means Bitcoin and, potentially, some additional set of sufficiently similar virtual currencies. We will also use "cryptocurrency" to denote the same.³⁷

Recommendation: In addition to the other recommendations below, which reflect needed clarification to the guidance in Notice 2014-21, the IRS should do one of the following:

- If the distinction between convertible and non-convertible virtual currencies is consequential for federal tax purposes, provide guidance on the tax consequences of non-convertible virtual currency as well as guidance on how taxpayers should determine if a given virtual currency is convertible or non-convertible; or,
- If the distinction is not consequential, clarify that Notice 2014-21 (as well as any additional clarifying guidance from the IRS) applies to the use of both convertible and non-convertible virtual currency.

Fair Market Value of Virtual Currency and Tax Basis of Virtual Currency Dispositions

This set of open questions bears on the methods taxpayers are permitted or required to use in calculating capital gains and losses resulting from virtual currency transactions and in determining the fair market value of tax-deductible virtual currency donations.

For a given property transaction made by a taxpayer, there are two tax determinations that need to be made: (1) whether the transaction resulted in a gain or a loss for the taxpayer, and (2) whether that gain or loss is a long-term capital gain/loss, a short-term capital gain/loss, or an ordinary gain/loss.

To determine whether a property transaction causes a gain or a loss, one must take the amount realized from the transaction—that is, the fair market value in U.S. dollars of the money and/or

³⁶ Internal Revenue Service, "IRS Virtual Currency Guidance," *IRS Notice 2014-21* (Apr. 14, 2014) at p.1, <https://www.irs.gov/pub/irs-drop/n-14-21.pdf>. Indeed, several foreign jurisdictions are considering the adoption of blockchain-based currency as legal tender. *See, e.g.*: Central Bank of The Bahamas, "Project Sand Dollar: The Central Bank Identifies Preferred Technology Solutions Provider for Bahamas Digital Currency," *Press Release* (Mar. 1, 2019) <https://www.centralbankbahamas.com/news.php?cmd=view&id=16540>; Daniel Palmer, "Eastern Caribbean Central Bank to Test Blockchain Legal Tender," *CoinDesk* (Mar. 6, 2019) <https://www.coindesk.com/eastern-caribbean-central-bank-takes-step-toward-digital-currency-roll-out>.

³⁷ For clarity, in addition to using its definition of "virtual currency," we also adopt Notice 2014-21's assumptions that "the taxpayer's functional currency is [] the U.S. dollar, the taxpayer [] use[s] the cash receipts and disbursements method of accounting and the taxpayer is [not] under common control with any other party to a transaction." Internal Revenue Service, "IRS Virtual Currency Guidance," *IRS Notice 2014-21* (Apr. 14, 2014) at p.2, <https://www.irs.gov/pub/irs-drop/n-14-21.pdf>.

other property the taxpayer receives from the sale or exchange—and subtract from it the taxpayer’s adjusted basis in the property being sold or exchanged.³⁸ The adjusted basis of an asset is, as one might expect, the asset’s basis as adjusted by various provisions of the tax code.³⁹

In general, the unadjusted basis of property is the cost thereof—the amount paid for the property in cash and/or other property.⁴⁰ When a taxpayer receives property in exchange for their services as an employee or contractor, the taxpayer is obliged to include the fair market value of the property as income in the year they receive it, and their basis in the property is equal to the recognized income.⁴¹

The determination of whether a gain/loss is a capital gain/loss depends on whether the property in question is a “capital asset” in the hands of the taxpayer. If it is a capital asset, then it will usually generate capital gains or capital losses; otherwise, it will generate ordinary gains or losses. In the tax code, capital assets are defined by exclusion—everything is a capital asset unless it falls under an excluded category such as inventory or accounts receivable for a taxpayer’s business.⁴²

As mentioned above, this report is focused on individuals’ use of Bitcoin and sufficiently similar cryptocurrencies. In that context, the virtual currency is unlikely to fall under an exclusion and, as a result, will be a capital asset in the hands of the taxpayer.⁴³ Such an asset generates either long-term or short-term capital gains or losses, depending on how long the property was held by the taxpayer before its sale or exchange. If the property was held for more than one year, it generates long-term capital gain/loss, which is subject to more favorable tax rates; if it was held for less than one year, it generates short-term capital gain/loss, which is taxed at the same rate as ordinary income.⁴⁴

³⁸ 26 U.S.C. § 1001(a).

³⁹ 26 U.S.C. § 1011 defines adjusted basis; several basis adjustments are codified at 26 U.S.C. § 1016 and implemented by regulation under 26 C.F.R. § 1.1016-1-6 & 1.1016-10.

⁴⁰ 26 U.S.C. § 1012. Basis is calculated differently for property included in inventory, acquired from a decedent, or acquired by gifts and transfers in trust (IRC 1013, 1014, and 1015 respectively).

⁴¹ 26 U.S.C. § 83(a). Technically, the fair market value of such property must be included in gross income in the year in which the rights of the taxpayer having the beneficial interest in the property are transferable or are not subject to a substantial risk of forfeiture, whichever occurs earlier, or, by election, at an even earlier date. 26 U.S.C. § 83(b). Further, the gross income recognized must be reduced by the fair market value of any money or property the taxpayer paid for the received property. 26 U.S.C. § 83(a). For clarity of presentation, these nuances are omitted above.

⁴² 26 U.S.C. § 1221(a).

⁴³ As IRS Publication 544 notes, “almost everything you own and use for personal purposes, pleasure, or investment is a capital asset.” Noncapital assets include business inventory (property held mainly for sale to customers) and assets used by a business to perform its trade or business. See: Internal Revenue Service, “Sales and Other Dispositions of Assets (For use in preparing 2018 returns),” *IRS Publication 544*, Cat. No. 15074K (Feb. 28, 2019) at p.22, <https://www.irs.gov/pub/irs-pdf/p544.pdf>.

⁴⁴ 26 U.S.C. § 1222 & 1223.

Open Question 2: How should taxpayers calculate the fair market value of virtual currency?

In many instances of the scenarios described above, the taxpayer needs to know the fair market value (FMV) of the property they are receiving or exchanging. This brings us to our next open question: How should taxpayers determine the FMV of virtual currency? Notice 2014-21 provides the following response to that question:

For U.S. tax purposes, transactions using virtual currency must be reported in U.S. dollars. Therefore, taxpayers will be required to determine the fair market value of virtual currency in U.S. dollars as of the date of payment or receipt. If a virtual currency is listed on an exchange and the exchange rate is established by market supply and demand, the fair market value of the virtual currency is determined by converting the virtual currency into U.S. dollars (or into another real currency which in turn can be converted into U.S. dollars) at the exchange rate, in a reasonable manner that is consistently applied.⁴⁵

This is a helpful start, but there are three significant gaps that need to be filled. First, most cryptocurrencies can be traded on more than one exchange, and the exchange rates across the different exchanges for a given cryptocurrency are not uniform. What should a taxpayer do when faced with different exchange rates at different exchanges? Second, taxpayers need more guidance on what the IRS will consider “a reasonable manner that is consistently applied.” Last, what does the IRS mean when they specify that taxpayers must determine the fair market value “as of the date of payment or receipt”? Cryptocurrency exchange rates often have significant intra-day volatility, and it is not immediately clear how the IRS expects, or will permit, taxpayers to calculate the FMV “as of the date of payment or receipt.”

Recommendation: The IRS should allow taxpayers to, for each cryptocurrency they use or possess, use either the exchange rate data from one exchange, averaged exchange rate data from a fixed set of exchanges, or a third-party exchange rate index, so long as they consistently use the same exchange, exchanges, or index to calculate the exchange rate for that cryptocurrency going forward. Taxpayers should also have the option to, for each cryptocurrency they possess, use an overall daily average exchange rate, a snapshot exchange rate taken at the same time of day each day, or the exchange rate at the time of transaction for each transaction, again so long as they consistently use their chosen methodology going forward.

These recommendations only bear on how the IRS interprets its existing guidance—adopting them would, arguably, not even require the publication of additional guidance. It is quite possible that a clearly articulated explanation of what the existing guidance means by

⁴⁵ Internal Revenue Service, “IRS Virtual Currency Guidance,” *IRS Notice 2014-21* (Apr. 14, 2014) at p.3 (“Q-5: How is the fair market value of a virtual currency determined?”) <https://www.irs.gov/pub/irs-drop/n-14-21.pdf>.

“reasonable manner that is consistently applied” and “as of the date of payment or receipt” would be sufficient to resolve the current uncertainty facing virtual currency-using taxpayers.

Open Question 3: How can taxpayers determine the cost basis of virtual currency dispositions?

In addition to clear guidance on what fair market valuation methods are acceptable, taxpayers need clarity on what tax lot relief⁴⁶ methods are available to them. A plain reading of the tax code and regulations suggests that the only permissible method for virtual currencies is specific identification, meaning that taxpayers need to, for each unit of virtual currency they possess, keep track of the date on which they acquired that virtual currency as well as their adjusted basis in it.⁴⁷ Then, every time the taxpayer transacts with virtual currency they must identify the specific unit of virtual currency with which they are transacting and use that specific unit’s adjusted basis, alongside its fair market value at the time or day of the transaction, to determine their gain or loss. Further, if the gain or loss is a capital gain or loss, then the taxpayer will need to compare the date on which they acquired that specific unit of virtual currency with the transaction date to determine whether their capital gain or loss is short-term or long-term.

In the case of Bitcoin, different bitcoins technically are nonfungible. In order to transfer ownership of a bitcoin to someone else, a user must create and broadcast a transaction to the network that uses, as its inputs, one or more specific previous transaction(s) in which the user received the bitcoin they wish to transfer. Keeping track of every unspent transaction they have received, the date they received it, and their basis in it, and then cross-referencing that information for every transaction they engage in is an incredibly onerous but technically feasible task for a Bitcoin user that holds their own private keys and uses a software wallet to transact. For those that use a hosted wallet, where the wallet provider has custody of the user’s private keys and transacts on their behalf, it may be effectively impossible for the taxpayer to adequately identify which specific previous transaction(s) a given transaction used as input(s), even if such identification is technically the only permissible method of determining the cost basis of the virtual currency disposition.⁴⁸

Treasury Regulation (Treas. Reg.) 1.1012-1 specifies that stocks and certain other securities are eligible for tax lot relief methods other than specific identification, such as FIFO (first-in,

⁴⁶ When a taxpayer has acquired multiple “lots” of the same asset over time, then the tax basis of each of those “tax lots” will be different to the extent that the fair market value of the asset changed in between purchases. When the taxpayer later disposes of some amount of that asset, in order to determine their basis in the asset they must first determine *which* tax lot the asset they sold came from. “Tax lot relief methods” refers to the different ways to go about making that determination.

⁴⁷ As noted above, this report is focused on taxpayers that use or invest in cryptocurrencies in a personal capacity. There are alternative methods of basis calculation available to other types of taxpayers. For example, businesses for which the virtual currency is classified as inventory can use the inventory methods of accounting under 26 U.S.C. § 471-475.

⁴⁸ Some other cryptocurrencies that may be subject to IRS Notice 2014-21 have technical differences that may impact this analysis as well. For example, Ethereum uses an account-based system rather than an unspent transaction output (UTXO) system.

first-out), but the IRS's current characterization of virtual currency does not appear to allow taxpayers to take advantage of them.⁴⁹ Treas. Reg. 1.6045-1 requires brokers and barter exchanges to file information returns on their customers' transactions in "covered securities."⁵⁰ In doing so, brokers are required to use various lot relief methodologies depending on the types of transactions in question and, in some instances, whether the customer has notified the broker of their election to use a different permissible lot relief method. The definition of "covered securities" used in Treas. Reg. 1.6045-1 is, essentially, any "specified security" that was acquired after a specified date.⁵¹ "Specified security" is, in turn, defined to consist of specific categories of stocks, debt instruments, options, and securities futures contracts.⁵² It is unlikely that a virtual currency would meet the definition of any of these categories.

However, the statutory language under which Treas. Reg. 1.6045-1 was written includes in the definition of specified security "any commodity . . . if the Secretary [of the Treasury] determines that adjusted basis reporting is appropriate for purposes of this subsection."⁵³ The Commodity Futures Trading Commission (CFTC), which oversees commodity futures markets, determined in late 2014 that virtual currencies are commodities.⁵⁴ It is likely that the IRS has statutory authority to, if it so chose, create information reporting requirements for virtual currency transactions of customers of brokers and barter exchanges that use, or permit, tax lot relief methods other than specific identification. Such an action would likely require a notice-and-comment rulemaking. The implementing regulations define "commodity" as "[l]ead, palm oil, rapeseed, tea, tin, or an interest in the foregoing[.]" "[a]ny type of personal property or an interest therein (other than securities as defined in paragraph (a)(3)) the trading of regulated futures contracts in which has been approved by the Commodity Futures Trading Commission[.]" and "[a]ny other personal property or an interest therein that is of a type the Secretary [of the Treasury] determines is to be treated as a 'commodity' under this section, from and after the date specified in a notice of such determination published in the Federal Register."⁵⁵ Virtual currency obviously does not fall under the first category. The second category is also problematic. Although there are regulated Bitcoin futures, none of them have been "approved" by the CFTC. Rather, they have gone through the CFTC's self-certification process, in which a "designated contract market" that plans to offer a new futures products files a "product self-certification submission" with the CFTC stating that the product does not violate any provision of the Commodities Exchange Act or the CFTC's regulations adopted

⁴⁹ 26 C.F.R. § 1.1012-1.

⁵⁰ 26 C.F.R. § 1.6045-1.

⁵¹ 26 C.F.R. § 1.6045-1(a)(15). The relevant date varies depending on the type of specified security being considered.

⁵² 26 C.F.R. § 1.6045-1(a)(14).

⁵³ 26 U.S.C. § 6045(g)(3)(B)(iii).

⁵⁴ See, e.g.: Commodity Futures Trading Commission, "CFTC Backgrounder on Oversight of and Approach to Virtual Currency Futures Markets," *CFTC Office of Public Affairs Release* (Jan. 4, 2018) https://www.cftc.gov/sites/default/files/idc/groups/public/%40customerprotection/documents/file/backgrounder_virtualcurrency01.pdf.

⁵⁵ 26 C.F.R. § 1.6045-1(a)(5).

thereunder.⁵⁶ Barring an objection from the CFTC, the designated contract market may then list the new product as soon as one day later without any need for explicit CFTC approval.⁵⁷ In order to expand the information reporting requirements of Treas. Reg. 6045-1, then, the IRS could look to the third category and publish a Federal Register notice stating that the Secretary of the Treasury has determined virtual currency is to be treated as a “commodity” for purposes of I.R.C. 6045 and Treas. Reg. 6045-1. Alternatively, the IRS could undertake a rulemaking to update the second category to reflect the existence of the self-certification process in such a way that causes Bitcoin to be included in the definition of “commodity” for purposes of I.R.C. 6045 and Treas. Reg. 6045-1, although this option would continue to exclude other, similar virtual currencies that the IRS may otherwise want to treat in the same manner as Bitcoin but for which there are not currently CFTC-approved futures contracts.

Recommendation: Given the difficulties of applying specific identification to virtual currency, and the fact that taxpayers conducting transactions in essentially any other commonly traded financial instrument have a variety of tax lot relief methods available to them, the IRS should allow taxpayers to use tax lot relief methods other than specific identification for virtual currency transactions. Taxpayers should be permitted to, if they so choose, elect to use different lot relief methods for each of their cryptocurrency “accounts”⁵⁸ in the same way they can select differing lot relief methods for eligible non-cryptocurrency accounts. This could be implemented through a rulemaking as described above, or through informal or formal guidance to taxpayers. If the IRS elects to accept this recommendation in a manner that requires notice in the Federal Register, we recommend both publishing a notice that virtual currency is to be

⁵⁶ See, e.g., Commodity Futures Trading Commission, “Self-Certification Filing Procedures,” *CFTC Website* (accessed April 2, 2019) <https://www.cftc.gov/IndustryOversight/ContractsProducts/ListingProcedures/index.htm>; Commodity Futures Trading Commission, “CFTC Backgrounder on Self-Certified Contracts for Bitcoin Products,” Fact Sheet (Dec. 1, 2017) https://www.cftc.gov/sites/default/files/idc/groups/public/@newsroom/documents/file/bitcoin_factsheet_120117.pdf.

⁵⁷ Commodity Futures Trading Commission, “CFTC Backgrounder on Self-Certified Contracts for Bitcoin Products,” Fact Sheet (Dec. 1, 2017) https://www.cftc.gov/sites/default/files/idc/groups/public/@newsroom/documents/file/bitcoin_factsheet_120117.pdf.

⁵⁸ The concept of a cryptocurrency “account” makes sense when a taxpayer uses a custodial wallet provider to secure their cryptocurrency, but breaks down when one considers cryptocurrencies that are self-custodied. Although there are technically no “accounts” in such a scenario, taxpayers should still be able to select different lot relief methodologies for different groups of assets. The ability to choose different tax lot relief methods on an account-by-account basis can be extended to the context of virtual currency by allowing the taxpayer to group, into one or more sets, the unspent transaction outputs (UTXOs) for which they control the private key. (Or, for more complex UTXOs, those for which they control a sufficient number of the associated private key(s) to create a transaction using the UTXO as an input.) So long as such grouping is done in a reasonable and consistently applied manner, we see no policy reason not to consider each grouped set to be an “account” for purposes of selecting lot relief methodologies. *For a technical treatment of Bitcoin transactions and UTXOs, see: Andreas M. Antonopoulos, Mastering Bitcoin: Unlocking Digital Currencies* at ch. 5. Sebastapol, CA: O’Reilly, 2014, available at <https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch05.html>.

treated as a “commodity” for purposes of I.R.C. 6045 and Treas. Reg. 6045-1 *and* undertaking a rulemaking to update the regulations to reflect the existence of the self-certification process.

Open Question 4: Do charitable donations of virtual currency resulting in a deduction of \$5,000 or more require a qualified appraisal?

Like other property, taxpayers that donate virtual currency to a charity are generally permitted to deduct the fair market value of the virtual currency or other property at the time of donation from their income that year.⁵⁹ However, this deduction is generally capped at \$500 unless the taxpayer satisfies certain documentation and substantiation requirements.⁶⁰ Donations for which the taxpayer claims a deduction of more than \$5,000 also require the documentation and submission of a qualified appraisal prepared by a qualified appraiser in accordance with generally accepted appraisal standards and other regulatory requirements.⁶¹ The tax code provides an exception to this appraisal requirement for certain “readily valued property” such as cash, stocks or other property held as inventory or primarily for sale to customers in the ordinary course of a trade or business, and securities for which market quotations are readily available on an established securities market.⁶²

As Notice 2014-21 recognizes, virtual currencies like Bitcoin are widely traded on a variety of exchanges from which pricing data is readily available. In this way, virtual currency is similar to the categories of “readily valued property” listed above. From a policy perspective, we should want a virtual currency donor to substantiate the fair market value of their donation using readily and widely available exchange data, which can be acquired at essentially no cost, rather than through a costly appraisal process.

However, most taxpayers are not engaged in a trade or business that entails, in its ordinary course, the sale of virtual currency to customers. In light of Notice 2014-21’s holding that virtual currency is not treated as currency that could generate foreign currency gain or loss for U.S. federal tax purposes, it is also unlikely that virtual currency would be considered cash for purposes of the appraisal exception.⁶³ Additionally, a prudent taxpayer would probably not decide to risk their deduction of more than \$5,000 being rejected by the IRS by attempting to use the appraisal exception afforded to “securities for which market quotations are readily available on an established securities market.”⁶⁴

Recommendation: We submit that the IRS should provide taxpayers with guidance explicitly allowing them to use readily available exchange data to value virtual currency donations in the

⁵⁹ 26 C.F.R. § 1.170A-1(a)-(c). There are a great many exceptions, adjustments, and caveats to this general statement that are not particular to virtual currency and which we do not discuss here.

⁶⁰ 26 U.S.C. § 170(f)(11)(A) and (B).

⁶¹ 26 U.S.C. § 170(f)(11)(C) and (D), and 26 C.F.R. § 1.170A-11(c).

⁶² 26 U.S.C. § 170(f)(11)(A)(ii)(I), 26 U.S.C. § 1221(a)(1), 26 U.S.C. § 6050L(a)(2)(B). “Readily valued property” also includes certain patents and other intangible property, as well as certain automobiles.

⁶³ Internal Revenue Service, “IRS Virtual Currency Guidance,” *IRS Notice 2014-21* (Apr. 14, 2014) at p.2 (“Q-2: Is virtual currency treated as a currency for purposes of determining whether a transaction results in foreign currency gain or loss under federal tax laws?”) <https://www.irs.gov/pub/irs-drop/n-14-21.pdf>.

⁶⁴ 26 U.S.C. § 6050L(a)(2)(B).

same way taxpayers are expected to use such data to calculate the fair market value of their virtual currency every other time they transact with it.

Forks and Air Drops

Bitcoin and similar cryptocurrencies are, fundamentally, a network of peers running software that executes a protocol to maintain and update a distributed ledger of transactions. If some subset of the network participants (Group A) begins to run software that is not compatible with the software being run by the rest of the network (Group B)—i.e., if the protocol Group A now uses would consider some transactions valid that Group B would consider to be invalid—then the cryptocurrency network will “fork” into two separate networks with two different distributed ledgers. After a fork, there would be two cryptocurrency networks, and two underlying cryptocurrencies. Anyone who owned units of the original network’s cryptocurrency would now own an equivalent number of tokens on *each* of the resulting networks.⁶⁵

In 2017, such a fork occurred on the Bitcoin network.⁶⁶ Disagreement over proposed technical changes to the Bitcoin core protocol resulted in a situation where a subset of the network changed their software in a way that was not backwards-compatible while the rest of the network did not. The two cryptocurrencies that resulted from this fork are Bitcoin (the branch of the fork that is generally considered to be the continuation of the original network) and Bitcoin Cash (the branch of the fork that is considered to be a new cryptocurrency that shares a common pre-fork history with Bitcoin). Anyone holding bitcoins prior to the fork would, after the fork, have an equivalent amount of both Bitcoin and Bitcoin Cash. By running software that implemented the unchanged Bitcoin protocol, they could transact with their bitcoin balance on the Bitcoin blockchain without any effect on the Bitcoin Cash blockchain; by running software that implemented the altered Bitcoin protocol, they could transact with their bitcoin cash balance on the Bitcoin Cash blockchain without any effect on the Bitcoin blockchain.

The fork that resulted in Bitcoin Cash received significant news coverage and attention, and it is unlikely that a typical Bitcoin user would have been unaware of its occurrence and, consequently, of the fact that post-fork they would have two distinct cryptocurrencies instead of one.⁶⁷ There are many forks, however, for which this is not the case. Developers frequently create forks of the Bitcoin (and other cryptocurrency networks’) blockchain to try out experimental features, to create a more customized version for a specific application, or to create a network with lower usage and, as a result, lower transaction costs.⁶⁸ Taxpayers who

⁶⁵ For a general discussion of how new cryptocurrency projects fork off from older ones, see: Peter Van Valkenburgh, “What are Forks, Alt-coins, Meta-coins, and Sidechains?” *Coin Center* (Dec. 8, 2015) <https://coincenter.org/entry/what-are-forks-alt-coins-meta-coins-and-sidechains>.

⁶⁶ “Bitcoin divides to rule,” *The Economist* (Aug. 5, 2017) <https://www.economist.com/finance-and-economics/2017/08/05/bitcoin-divides-to-rule>.

⁶⁷ Pete Rizzo, “Will Bitcoin Cash Impact the Bitcoin Price? Traders Split on Possible Fork,” *CoinDesk* (Jul. 31, 2017) <https://www.coindesk.com/will-bitcoin-cash-impact-bitcoin-price-traders-split-possible-fork>.

⁶⁸ See, for example, *Litecoin*: Danny Bradbury, “Litecoin: Origins and potential of the world’s second largest cryptocurrency,” *CoinDesk* (Jul. 23, 2013) <https://www.coindesk.com/litecoin-founder-charles-lee-on-the-origins-and-potential-of-the-worlds-second-largest-cryptocurrency>.

have owned a well-known cryptocurrency such as Bitcoin for any length of time have the ability, if they download the appropriate software for the forked network in question, to sell or spend tokens on multiple cryptocurrency networks resulting from forks in the Bitcoin blockchain that have occurred in the time they have been holding bitcoin. Many of those tokens would be worth very little, and the taxpayer likely has no idea that most of them exist, but they inarguably represent value that can only be accessed by the taxpayer.

A distinct but similar concept to a network fork is an “airdrop.”⁶⁹ Suppose you are a developer with a great idea for a cryptocurrency network. The protocol you envision for your new cryptocurrency uses public-private key pairs, like Bitcoin, but is otherwise very different. You want to get your cryptocurrency into the hands of users to drive network effects. One way you could do this is to fork the Bitcoin blockchain—that way, everyone who had bitcoin at the moment of the fork would, after the fork, also have tokens on your new network. You could also try to sell the tokens, or you could give them away for free. One way to give away tokens for free is via an airdrop. In an airdrop, the developers of a (usually new) cryptocurrency network download a copy of the Bitcoin (or other cryptocurrency network) blockchain, add up how many bitcoin are currently held at each public address on the Bitcoin network, and then, for each such public address, allocate a commensurate amount of tokens to that address on the blockchain of the network they are developing. This allows the developers to widely distribute the tokens to people who they know are cryptocurrency users without forking any extant network. Some airdrops are opt-in, where there is a period of time during which persons wanting to receive airdropped tokens must affirm that fact, and then the airdrop is performed by distributing new tokens in proportion to the relative Bitcoin balances of those who have opted in. Other airdrops are done without any input, and often without any awareness, of the token recipients.

Open Question 5: What is the tax treatment of virtual currency tokens received from network forks and air drops?

In many cases, for a given fork or airdrop and a given Bitcoin user, the user may be wholly unaware of the existence of the new network and the coins on that network over which they have control. Other times, the recipient might decide to dispose of the token immediately by, *inter alia*, selling it for fiat on a custodial exchange. Or, the recipient might hold on to the token for a period of time before disposing of it. In other words, there are four main scenarios to consider:

1. Recipient is aware of new token, and promptly uses their private key to take control of it and sell it.
2. Recipient is aware of new token, but decides to hold onto it until a future date. On that future date, they sell the token.
3. Recipient is initially unaware of the token; on a later date, recipient becomes aware of the token and sells it.

⁶⁹ Although the description of airdrops here captures the important concepts for the topic at hand, it omits significant technical details and should not be relied upon more broadly.

4. Recipient never accesses the new token.

In each situation, there are several pertinent tax questions:

1. What is the recipient's basis in the tokens received?
2. When is the recipient allowed, and when are they required, to recognize income as a result of receipt of the new tokens?
3. What type of income is realized?
4. To the extent that the type of income realized is a capital gain, what date should the recipient use to calculate whether or not the capital gain is long- or short-term?

Recommendation: If the recipient does not exercise dominion over and dispose of the tokens, there should be no tax effect. If the recipient does take control of and disposes of the tokens, income should generally be recognized at the time of disposition. The type of gain realized should depend on the classification of the asset in the hands of the taxpayer, but would generally be a short-term capital gain. For tokens received as the result of a network fork, the taxpayer should be allowed to distribute their adjusted basis in the pre-fork token between the two resulting post-fork tokens. For purposes of calculating the holding period of the post-fork tokens to determine if a gain is short- or long-term, the taxpayer should include the time they held the pre-fork token. If a taxpayer holds their cryptocurrency with a custodial exchange, any actions that the exchange takes regarding airdropped or forked tokens should not affect the taxpayer unless such actions were undertaken at the direction of the taxpayer.

Reports of Foreign Financial Accounts

Notice 2014-21 states that virtual currency payments are subject to the same reporting requirements as any other payment made in property.⁷⁰ Two such annual reporting requirements are the Report of Foreign Bank and Financial Accounts and the Statement of Specified Foreign Financial Assets.

Open Question 6: What are the reporting requirements for virtual currencies under FBAR and FATCA?

Under federal regulation, each United States person that has a financial interest in, or authority over, a bank account, securities brokerage account, or other financial account in a foreign country that exceeds certain thresholds is required to annually submit to the Treasury Department via the IRS FinCEN Form 114, Report of Foreign Bank and Financial Accounts (FBAR).⁷¹ Specifically, if a United States person had a financial interest or authority over at least one financial account located outside of the United States in a tax year, and at some point during the year the aggregate value of all such foreign financial accounts held by that person

⁷⁰ Internal Revenue Service, "IRS Virtual Currency Guidance," *IRS Notice 2014-21* (Apr. 14, 2014) at p.5 ("Q-12: Is a payment made using virtual currency subject to information reporting?") <https://www.irs.gov/pub/irs-drop/n-14-21.pdf>.

⁷¹ 31 C.F.R. § 1010.350.

exceeded \$10,000, then they must complete and submit FinCEN Form 114 to the IRS.⁷² Virtual currencies held in a custodial account located outside of the United States—either because they are held with a foreign financial institution or with a foreign branch of a U.S. financial institution—may or may not need to be reported under FBAR, depending on the IRS and FinCEN’s interpretation of whether such holdings constitute a “reportable account” for purposes of FBAR.⁷³

The Foreign Account Tax Compliance Act (FATCA) places various reporting and withholding requirements on financial intermediaries and requires individual taxpayers holding more than \$50,000 in “specified foreign financial assets” to report information about those assets by submitting IRS Form 8938, Statement of Specified Foreign Financial Assets, alongside their annual tax return.⁷⁴ In December 2014, the IRS requested comment on the proper treatment of virtual currencies under FATCA reporting requirements.⁷⁵ Since that 32-word request for comment, the IRS has not issued further information requests or guidance.

Broadly, the “specified foreign financial assets” in question under FATCA are made up of four types of financial assets: (1) financial accounts maintained by a foreign financial institution; (2) stocks and securities issued by someone other than a U.S. person; (3) financial instruments or contracts held for investment that have an issuer or counterparty other than a U.S. person; and (4) financial interests in foreign entities.⁷⁶ Virtually currencies held in the custody of a financial institution that is not based in the United States may meet the definition of category (1), although there is a colorable argument that they do not. Digital assets that are deemed stocks or securities for federal tax purposes, and for which the issuer is someone other than a U.S. person, likewise would qualify as specified foreign financial assets for FATCA purposes. Last, it is possible that blockchain-based derivatives, and potentially some smart contracts, would qualify as specified foreign financial assets if there is a counterparty to the transaction and that counterparty is someone other than a U.S. person.⁷⁷

Recommendation: The IRS should clarify whether and when virtual currency holdings and payments are subject to reporting requirements under FATCA and FBAR. Because such clarification would be an explanation of how existing reporting requirements apply to virtual currencies, it would likely not require a notice-and-comment rulemaking.

⁷² 31 U.S.C. § 5314. Instructions and additional information for FinCEN Form 114 are available at <https://www.irs.gov/businesses/small-businesses-self-employed/report-of-foreign-bank-and-financial-accounts-fbar>.

⁷³ 31 C.F.R. § 1010.350(c).

⁷⁴ 26 U.S.C. § 6038D. In the implementing regulations, there are higher thresholds for married individuals filing a joint return and for individuals living abroad. 26 C.F.R. 1.6038D-2(1) through (4).

⁷⁵ Internal Revenue Service, “Internal Revenue Bulletin,” *IRS Bulletin No. 2014-53* (Dec. 29, 2014) pg. 984, <https://www.irs.gov/pub/irs-irbs/irb14-53.pdf>; Reporting of Specified Foreign Financial Assets, 79 Fed. Reg. 73817 (Dec. 12, 2014) <https://www.federalregister.gov/documents/2014/12/12/2014-29125/reporting-of-specified-foreign-financial-assets>.

⁷⁶ 26 U.S.C. § 6038D.

⁷⁷ 26 C.F.R. § 1.6038D-3(b).

Conclusion

It has been over a decade since the IRS's Taxpayer Advocate noted the open questions regarding taxation of virtual worlds and economies and admonished the agency to "produce specific early guidance on difficult issues confronted by taxpayers on a regular basis in emerging areas of economic activity. Otherwise, it risks turning these taxpayers into unintentional tax cheats, establishing noncompliance norms in the industry, and leaving IRS employees without clear guidance about how to do their jobs."⁷⁸ The only piece of guidance the IRS has released to date, a six-page FAQ,⁷⁹ does not satisfy this mandate; this has been noted by stakeholders both internal, such as the Treasury Inspector General for Tax Administration⁸⁰ and the Information Reporting Program Advisory Committee,⁸¹ and external, such as the American Institute of Certified Public Accountants⁸² and the American Bar Association.⁸³ While it is understandable that the IRS has been slow to tackle these issues given their complexity and the agency's limited resources, it is unacceptable that it appears to be ramping up enforcement efforts against "[t]axpayers who do not properly report the income consequences of virtual currency transactions,"⁸⁴ without ever having made clear what it means to "properly report."

This report has laid out several of the most pressing ambiguities facing U.S. taxpayers that use cryptocurrencies as well as common-sense approaches to resolving them. Our hope is that the IRS will look to them as a starting point for additional guidance in this space, and will refrain from taking legal action against well-meaning cryptocurrency users who simply do not know how they are supposed to account for these new digital assets when they file their tax returns.

⁷⁸ James R. White, et al., "Virtual Economies and Currencies, Additional IRS Guidance Could Reduce Tax Compliance Risks," *Government Accountability Office Report to the Senate Committee on Finance (GAO-13-516)* (May 2013) <https://www.gao.gov/assets/660/654620.pdf>.

⁷⁹ Internal Revenue Service, "IRS Virtual Currency Guidance," *IRS Notice 2014-21* (Apr. 14, 2014) <https://www.irs.gov/pub/irs-drop/n-14-21.pdf>.

⁸⁰ Treasury Inspector General for Tax Administration, "As the Use of Virtual Currencies in Taxable Transactions Becomes More Common, Additional Actions Are Needed to Ensure Taxpayer Compliance," *TIGTA Report No. 2016-30-083* (Sep. 21, 2016) <https://www.treasury.gov/tigta/auditreports/2016reports/201630083fr.pdf>.

⁸¹ Dennis Ventry, Jr., et al., "Information Reporting Advisory Committee Public Report," *IRS Publication 5316*, Catalog Number 71824A (Nov. 2018) at pp. 75-76, <https://www.irs.gov/pub/irs-pdf/p5316.pdf>.

⁸² American Institute of CPAs, "Request for Guidance Regarding Virtual Currency," *Public Interest Comment from the AICPA to the IRS* (May 30, 2018) <https://www.aicpa.org/content/dam/aicpa/advocacy/tax/downloadabledocuments/20180530-aicpa-comment-letter-on-notice-2014-21-virtual-currency.pdf>.

⁸³ American Bar Association Section of Taxation, "Comments on Notice 2014-21," *Public Interest Comment from the ABA to the IRS* (March 24, 2015) <https://www.americanbar.org/content/dam/aba/administrative/taxation/policy/032415comments.pdf>.

⁸⁴ Internal Revenue Service, "IRS reminds taxpayers to report virtual currency transactions," *IRS News Release IR-2018-71* (Mar. 23, 2018) <https://www.irs.gov/newsroom/irs-reminds-taxpayers-to-report-virtual-currency-transactions>.



Exchanges call for greater regulatory clarity at IRS crypto tax summit



by [Michael McSweeney](#)

March 3, 2020, 2:37PM EST · 2 min read

Quick Take

- The U.S. Internal Revenue Service is hosting crypto industry representatives and agency officials for a tax summit focused on the tech
- The second of four panels centered on exchanges
- Tax execs from Coinbase and Kraken had a straightforward message: we want more clarity.

Representatives for two cryptocurrency exchanges called for greater regulatory clarity from the Internal Revenue Service (IRS) during a Tuesday event at the U.S. tax authority's headquarters in Washington, D.C.

During an IRS Virtual Currency Summit panel focused on exchange issues, the audience – comprised of industry stakeholders and IRS officials – heard from Coinbase head of global tax information reporting Sulolit Mukherjee and Kraken head of global tax Lisa Askenazy Felix. Also appearing on the panel was Jamison Sites, Washington national tax manager for RSM Tax LLP as well as John Cardone, assistant deputy commissioner for compliance integration.

Still, Mukherjee struck a positive note given the very existence of the event itself, commenting: "I think the willingness of the IRS to engage us in conversations like this is a very healthy sign."

Front-and-center during the panel: that crypto exchanges want more clarity from the IRS, both in terms of what their business requirements are under U.S. laws and the exact steps they need to take to meet them.

Indeed, Cardone acknowledged that there is "uncertainty" among relevant parties on the issue of exchange reporting and a lack of specificity on certain topics, including which forms should be issued to users.

Part-and-parcel to that notion was an emphasis on the nascent nature of the crypto industry. Comments during the panel show concerns that a beefed-up regulatory regime might prove burdensome to exchanges – particularly those that are spending time and money to remain compliant with U.S. rules.

"I think most of us in the room would agree that there is no clarity," Askenazy Felix remarked.

RSM's Sites noted that his firm tells clients to "do your best," given the existing guidance from the IRS.

"This is really a drive to increase self-reporting and self-compliance," he remarked.

With an eye to the future, exchange panelists were asked whether they might support the development of a central repository of exchange data that would both standardize that information as well as providing access to law enforcement.

Both Askenazy Felix and Mukherjee largely rejected the idea, with Askenazy Felix remarking: "We would not be in favor of wholesale providing our information, all of our client information, to any centralized database." She cited privacy and security issues, pointing to the risk that such a repository could be hacked and, as a result, lead to the theft of sensitive data.

Such an approach "poses many challenges," according to Mukherjee.

On the question of whether exchanges themselves might offer tax reporting-related services, Felix said that Kraken is looking at providing such an offering, but that this move isn't set in stone.

One final point raised during the panel was on the question of flexibility if exchanges – assuming they are provided with specific guidance in the future – move to become compliant over time. "That is the danger here, as we are a very emerging, nascent industry, that you're going to push operation offshore," said Askenazy Felix.



TESTIMONY OF

Peter Van Valkenburgh¹

Director of Research at Coin Center

BEFORE THE

United States Senate Banking Committee

“Exploring the Cryptocurrency and Blockchain Ecosystem”

October 11, 2018

Executive Summary

You may have heard that “blockchain technology” is the solution to any number of social, economic, organizational, or cybersecurity problems. *It is not.* A blockchain is merely a data structure and “blockchain technology” is a vague and undefined buzzword. In this paper, we explain the true technologies that undergird blockchain networks and the distinctions between public and private blockchain networks, why they matter, and why only public blockchain networks can solve certain specific issues related to electronic cash, identity, and the Internet of Things.

“Blockchain technology” is not a helpful phrase. It abstracts real, specific technical innovations into a generalized panacea. The phrase suggests a vague design pattern, which is then trumpeted as the solution to all manner of societal and organizational problems. And amongst all of this cheerleading, almost nothing is ever offered in the way of real design specifics. This tends to be because “**blockchain technology**” is described monolithically, as if there are no specific design choices to be made in building “blockchain solutions” beyond choosing to use a blockchain. The advantages and disadvantages of various approaches and technical architectures are generally not discussed (except perhaps by experts) and the non-technical public is left with a warm blanket and little understanding of why any of this matters.

This testimony offers specifics. It begins by describing why “**decentralized computing**” matters. If all of the “blockchain technology” hype has one thing in common, it’s the idea that *a computer application, which creates some useful result for its users, can be run*

¹ Peter is Director of Research at Coin Center, the leading independent non-profit research and advocacy group focused on the public policy issues facing cryptocurrency technologies such as Bitcoin. This testimony is based largely on a report published by Coin Center. See Peter Van Valkenburgh, “Open Matters: Why Permissionless Blockchains are Essential to the Future of the Internet” *Coin Center* (2016) <https://coincenter.org/entry/open-matters>.

simultaneously on many computers around the world rather than on just one central server, and that the network of computers can work together to run the application in a way that avoids trusting the honesty or integrity of any one computer or its administrators. To describe this idea we prefer the term “decentralized computing” to “blockchain technology,” because it is more descriptive and it is also a broader category.

This testimony demystifies the actual technologies behind “blockchain technology” and explains these *several* technologies in a way that even non-technical readers will understand. This testimony creates a typology of “blockchain technologies” and it will suggest that only certain *types* of “blockchain technology” can be real solutions to certain major social and organizational challenges.

For starters, rather than talking about “blockchain technology” in the abstract, we discuss the real technical innovations that underlie Bitcoin, the actual functioning technology that has spurred all the blockchain hype. There are really **three core innovations** that underlie Bitcoin: **peer-to-peer networking, blockchains, and consensus mechanisms**. Of these, peer-to-peer networking is generally nothing new, and blockchains are merely novel ways of storing and validating data. **Consensus mechanisms, however, are the truly disruptive, interesting, and critical component of the design.** When it comes to capabilities, risks, and disruptive potential, however, **not all consensus mechanisms are created equal**. The critical nature of consensus mechanisms in these new blockchain-powered decentralized computing systems, and the variability in types of consensus mechanism design are why the bulk of this testimony focuses on explaining consensus mechanisms to non-technical audiences.

In general, **by consensus we simply mean the process by which a number of computers come to agree on some shared set of data and continually record valid changes to that data.** So the blockchain might be the form that the data take, *e.g.* a hashed list of valid transactions in bitcoin, but it is the consensus mechanism that generates that blockchain, validates the data, and continually keeps the data updated and reconciled between all of the computers in the system.

This brings us to the question of “publicness” in the consensus mechanism. Who is allowed to read the data over which the network is forming consensus, and possibly more important, who is allowed to participate in the process that ultimately results in new data being added? Are some consensus mechanisms more open to free participation than others? **In a public consensus mechanism anyone with a computer and an internet connection should be eligible to play a role in writing consensus data; in a private consensus mechanism only those who have been identified by a centralized authority and given an authorization credential are allowed to participate.**

The operation of various consensus mechanisms is described in the full testimony. Public consensus mechanisms include **proof-of-work** based mechanisms, as found in Bitcoin and most cryptocurrencies, as well as **proof-of-stake** mechanisms and **social consensus** mechanisms. Private consensus mechanisms generally follow what we call a **consortium consensus** model, wherein only identified and credentialed consortium members share the privilege of writing consensus data.

From an **innovation policy** perspective, public consensus mechanisms are superior to their

private counterparts because they create purpose-agnostic platforms atop which anyone with a connected computer can build, test, and run user-facing decentralized applications. In this sense, **networks powered by public consensus mechanisms mirror the early Internet, and may one day become as indispensable as the Internet in facilitating free speech, competition, and innovation in computing services.**

Apart from publicness, we also discuss the nature of **trust** and **privacy** in each of the several consensus mechanisms. Public consensus mechanisms demand that users place trust in unknown third parties who are economically motivated to behave honestly because they have **skin in the game** and face **competitive pressures**. Private consensus mechanisms demand that users place trust in the identifying authority who provisions consortium members with credentials, and the honesty and cybersecurity practices of the members themselves. Public consensus mechanisms trade **transparency** for **privacy** but new technologies such as **zero-knowledge proofs** and **homomorphic encryption** may enable public networks to have superior privacy and verifiability as compared with private networks that rely only on **perimeter security** to maintain privacy.

Finally, we explain why public consensus mechanisms, specifically, are critical for three particular decentralized computing applications: **electronic cash, identity, and the Internet of Things.**

- **Electronic Cash.** Truly electronic *cash* (i.e. fungible bearer assets, the use of which resembles that of paper notes) offers **efficiencies that existing electronic money transmission systems cannot**. There are hidden costs to legacy systems: chargebacks, and transactions forgone because fees are greater than the value being sent or because participants cannot obtain a banking relationship. Fundamentally, from a user's perspective, a private-blockchain money transmission technology doesn't "just work" from the get-go. I cannot send or receive money until I open an account and establish a legal relationship with a company. This may be a tolerable inconvenience, but it is not a system that works like cash, which can be accepted in the hand without any prior arrangements in place. **Only public consensus mechanisms, by fully automating the creation and maintenance of a ledger according to pre-established rules and economic incentives, can offer electronic transactions that are as good as cash.**
- **Identity. The Internet lacks a native identity layer.** This shortcoming is the reason why Internet users must rely on a tapestry of weak passwords, secret questions, and knowledge of mothers' maiden names to verify their identity to various web service providers. The need for a better solution is widely recognized, and **by creating a shared and unowned platform for recording identity data, public blockchains may provide the answer.**
- **The Internet of Things.** Firstly, public blockchain networks allow for a truly decentralized data structure for device identity (I am a bulb in this home's kitchen) and user access authorization (the user with address 0xE1A... is the only person who can turn me on and off). The redundant and decentralized nature of data on these networks can ensure that these systems have true longevity, and that **a manufacturer's decision to end support for a product will not destroy the user's ability to securely access the product's features.**

Secondly, **public blockchain networks can help ensure that devices are interoperable and compatible** because critical infrastructure for device communication, data storage, and computation can be commoditized and shared over a peer-to-peer network rather than be owned (as a server warehouse is owned) by a device manufacturer that may be reticent to opening its costly platform to competitors.

Lastly, **device payments for supporting and maintaining that networked infrastructure or allowing the device's user to easily engage in online commerce can be made efficient** by utilizing the electronic cash systems that only public consensus mechanisms can facilitate.

A public consensus mechanism decentralizes trust, spreading out power on the network across a larger array of participants. For any use-case, this decentralization helps ensure **user sovereignty, interoperability, longevity, fidelity, availability, privacy, and political neutrality**. In the full testimony, the necessity of these attributes is explained in the context of each decentralized computing application (electronic cash, identity, and the Internet of Things), and a discussion of public and private consensus mechanisms for that application follows.

Contents

Executive Summary	1
I. The Decentralized Computing Revolution	6
A. An Easy Introduction to Decentralized Computing	6
B. Platforms for Innovation: Computing, Sharing, Trusting	9
C. Platforms for Innovation: Public or Private	11
D. The Internet and Permission	13
II. Making Sense of Consensus	15
A. Proof-of-Work	17
B. Proof-of-Stake	21
C. Consortium Consensus	22
D. Social Consensus	23
III. Publicness, Trust, and Privacy Across Various Consensus Models	23
A. Publicness Across Consensus Mechanism	24
B. Trust Across Consensus Mechanisms	28
C. Privacy Across Consensus Mechanisms	35
IV. Use Cases in which Public Consensus is Critical	44
A. Electronic Cash	45
B. Identity	52
C. The Internet of Things	58
V. Conclusion	67

I. The Decentralized Computing Revolution

If all of the “blockchain technology” hype has one thing in common, it’s the idea that a computer application, which creates some useful result for its users, can be run simultaneously on many computers around the world rather than on just one central server, and that the network of computers can work together to run the application in a way that avoids trusting the honesty or integrity of any one computer or its administrators. To describe this idea, we prefer the term “decentralized computing” to “blockchain technology,” because it is more descriptive and it is also a broader category.

A. An Easy Introduction to Decentralized Computing

The easiest way to understand decentralized computing is to begin by thinking about a computer program you use and with which you are comfortable. It could be any computer program that you use for work or for fun. For this example, let’s just pick a *word processor*. Sure it’s not the most titillating software out there, but pretty much everyone who has ever used a computer has used a word processor at some point in their digital lives.

Let’s think about the history of the word processor. In the *old* days—the 1990s no less—word processing, like dying, was something you always did alone. If you used Microsoft Word, Wordperfect, or MacWrite, you were running software that used *only* the processor, memory, disk space, monitor, and keyboard of *your personal computer*. The word processor was software trapped on an island. If you wanted to share your draft for the next great American novel, then you would either need to print it or save it as a file on a disk and hope your editor, reader, or critic had the same word processing software as you and could open the file on her own island-like computer. If she made edits she would need to send the file back and you would need to merge her changes with any changes you had made since she got a copy. Frustrating, but a real improvement over piles of redlined paper.

Fast forward to the 21st century and new word processing applications began to make collaboration easier, most notably Google Docs and Microsoft Word with OneDrive. These new services took advantage of what marketing executives persuasively and reassuringly dubbed “the cloud.” Word processing via the cloud means it is much easier to work with others in creating a document; in the best implementations you can control who has read or write access, see your co-authors typing in real time, comment and discuss changes, and see a full history of everyone’s edits.

From a computing standpoint this is not cloud magic. What is really happening is that the word processor software is no longer running on your island-like computer; it is running on a server that Google or Microsoft owns and maintains somewhere in a giant warehouse somewhere in the world. The interface that we see on our computers when we use these services is just that, an interface—a way to communicate with the computer that Google or some other cloud services provider owns and controls. Collaboration is a cinch with these systems because every editor can have an interface that talks to the same central computer.

The software is still running on an island, but it's an island that everyone can connect to.

Decentralized computing systems now under development present a new opportunity. Rather than moving the computation from the user's device to a centralized server in order to facilitate collaborative applications like Google Docs, we could instead replicate the computation across the otherwise island-like computers of all users.

Imagine I've got an idea for the next hit young adult novel about dragons, and I have a co-author/by-day-herpetologist who is great at describing the scales, a cold-blooded editor at Penguin who is ready to viciously rip apart our draft, and a family of dragon-enthusiast sons, daughters, nieces, and nephews who are the ideal focus group for dragonian feedback. How can we all work together to get this dragon tale off the ground? Rather than all of us connecting to a central server to view and edit the shared draft, we could have all our computers connect to each other in a decentralized web, and our computers could work together to agree upon, and stay in sync with, the latest draft, edits, discussions, and permissions describing who is allowed to edit, comment, or read.

That is decentralized computing: the ability to run applications not on your own island-computer or on someone else's central computer, but on a truly nebulous cloud computer not owned or controlled by any single party.

Our word processing example has now, however, reached the end of its usefulness. As the PC and the Internet proved, it is not a single application like word processing that forges the value of today's information superhighway. The value is in the highway itself: a general purpose computing platform, full of cars, buses, vehicles of all types and colors helping people reach all sorts of destinations. As discussed in the next section, the development of these purpose-agnostic platforms is the true decentralized computing revolution at hand.

B. Platforms for Innovation: Computing, Sharing, Trusting

The PC and the Internet were revolutionary not because they were self-contained innovations, but rather because they were platforms for innovation. Decentralized computing tools like Bitcoin and Ethereum, discussed throughout, are the beginnings of a new platform for innovation that promises to facilitate a third wave of computing. The PC gave us home computing and productivity applications; the Internet gave us networked computing, collaboration, and rich audio-visual communication; and decentralized computing will give us tools to enable trust, exchange, and community governance.

The PC enabled a wave of consumer and professional applications, from word processing to gaming, from music production to 3D design. Abruptly, the child of a middle income household had a printing press, a cavernous arcade, a recording studio, a suite of architectural drafting tools and paper, and more at her fingertips in a box that sat inconspicuously in her parents' home office.

Then the Internet allowed these otherwise isolated productivity tools to be networked, to

speak to the world. The PC ran applications, and the Internet enabled those applications to communicate globally, to be multi-user, to share data. Now the home printing press was matched with a fleet of newspaper delivery trucks; the arcade, still cavernous, was open to players across the world who could compete with each other; the recording studio came with a record label, trucks to ship vinyl, and stores to sell hits; the architectural tools came with virtual warehouses of objects, furniture, homes, and vehicles waiting to be built or even printed in 3D.

The Internet created a uniform mechanism for computers to speak to each other, but it did not create a uniform mechanism for verifiable agreement (what we might call “trust”) between two or more computers and their two or more users. As cryptographer Nick Szabo has written:

When we currently use a smartphone or a laptop on a cell network or the Internet, the other end of these interactions typically run on other solo computers, such as web servers. Practically all of these machines have architectures that were designed to be controlled by a single person or a hierarchy of people who know and trust each other. From the point of view of a remote web or app user, these architectures are based on full trust in an unknown “root” administrator, who can control everything that happens on the server: they can read, alter, delete, or block any data on that computer at will.²

We have come to call shared computing tools “cloud computing,” but, marketing aside, *there is no cloud, there’s just other people’s computers*. So when, today, we engage in any sort of shared computing—whether it be social networking, collaborative document editing, shopping, online banking, or posting a video of our pets—we are utilizing the computers of an intermediary—whether it be Facebook, Google, Amazon, Bank of America, or YouTube respectively. Those intermediaries have control over everything that happens on their servers. They can see a wealth of our personal data and users trust them to only use and manipulate that data according to user instructions and in the best interest of users. Any agreement or level of trust between two users of a given intermediary’s service—as when I sell my car to another eBay user, or recognize the positive eBay feedback and reputation of the prospective buyer—is established and maintained by that intermediary.

This architecture has been essential to the rise of the Internet and collectively we have benefited tremendously from the creation of these shared computing systems. It does, however, introduce a great deal of trust into consumer-business relationships; trust that can be misplaced and abused if an intermediary maliciously misuses their customer’s data, fails to

² Nick Szabo, “The dawn of trustworthy computing” *Unenumerated* (Dec. 2014) <http://unenumerated.blogspot.com/2014/12/the-dawn-of-trustworthy-computing.html>. See also IBM Institute for Business Value, *Device Democracy: Saving the future of the Internet of Things* <https://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03620usen/GBE03620USEN.PDF> (“The Internet was originally built on trust. In the post-Snowden era, it is evident that trust in the Internet is over. The notion of IoT solutions built as centralized systems with trusted partners is now something of a fantasy. Most solutions today provide the ability for centralized authorities, whether governments, manufacturers or service providers to gain unauthorized access to and control devices by collecting and analyzing user data.”).

secure it from hackers, or profits unfairly from a user who is locked into the service and finds it difficult to migrate their data to a competing service provider.

New and emerging computing architectures can help forge trustworthy relationships directly between users without intermediaries. The most visible of these new systems thus far is Bitcoin, a peer-to-peer network protocol that allows users to hold and send provably scarce tokens (bitcoins) that can function like cash for the Internet. Electronic cash, however, is just one potential computing service that can be designed to be intermediary-less, to run across the computers of a decentralized network of users rather than on the centralized servers of a particular service provider.

At root, any shared computing system can be thought of as a single shared computer, a computer made up of computers. Bitcoin is, following this logic, a computer made up of many computers whose several users have installed and are running Bitcoin-compatible software. Working together, all of these computers periodically come to an agreement over the ledger of all Bitcoin transactions—the Bitcoin blockchain. That ledger is, at any moment, the authoritative “state” of the decentralized Bitcoin computer. But computer “state” can be any data, not just a list of cash-like transactions. For example, when using Microsoft Word, a writer is perpetually updating the state of her computer, typing word after word into a document whose current changes—the current state—continually appear on the screen.

If a decentralized network of computers can continuously agree on the most recent and updated state of all interactions on that network—like keystrokes to a Word document—then it could be programmed to perform the computations necessary for any number of applications. Tracking the reputation of sellers and buyers, permissioning editing or access rights to a shared document, rewarding creative contributors for popular video content, any of the previously described “cloud” services provided by intermediaries could be programmed into a decentralized computing network. As Szabo has noted,

Much as pocket calculators pioneered an early era of limited personal computing before the dawn of the general-purpose personal computer, Bitcoin has pioneered the field of trustworthy computing with a partial block chain computer. Bitcoin has implemented a currency in which someone in Zimbabwe can pay somebody in Albania without any dependence on local institutions, and can do a number of other interesting trust-minimized operations, including multiple signature authority. But the limits of Bitcoin's language and its tiny memory mean it can't be used for most other fiduciary applications[.]³

Several efforts are underway to design systems that can enable a larger range of “fiduciary” applications, systems that will be effectively *general purpose decentralized computers*: platforms for trustworthy shared computing just as flexible and repurposable as the PC and the Internet have become. Some of these systems modify or build on top of Bitcoin (Rootstock⁴ and

³ *Id.*

⁴ Sergio Demian Lerner, *RSK Rootstock Platform: Bitcoin Powered Smart Contracts* (Nov. 2015)

Blockstack⁵ among others), others are new standalone network protocols (the largest by value is Ethereum⁶). Still others are building decentralized computing systems that are private or permissioned by default (most notably Corda by R3CEV⁷), in order to allow a pre-specified set of users to agree upon some limited-purpose computation—like validating contracts between banks.

The component parts of these new architectures are generally three-fold: peer-to-peer networking, blockchains, and consensus mechanisms. All three of these concepts are often lumped together under the general and impressive-sounding heading “blockchain technology,” but for clarity this testimony will deal with each separately and will ultimately focus on the third lump—consensus mechanisms—because it is the architecture of this third component that has the most important implications for building useful and well-functioning decentralized applications.

You can think of these three technologies as follows: *peer-to-peer networking* is how connected machines communicate with each other, *blockchains* are the data structures the connected peers use to store important variables in the shared computation, and the *consensus mechanism* is the tool to generate the shared and agreed-upon computation itself.

As we will discuss, the architecture of the consensus mechanism is important to consider. Different choices may have different outcomes for users—more or less privacy, more or less choice, more or less costs to participation. Just as the fundamental technical architecture of the PC and the Internet had long-term ramifications for the relative fairness, distribution and availability of computing and communication tools, so may choices in the now-unfolding architecture of consensus.

As we will explain, *all* new approaches to decentralized computing—whether private or public—should be celebrated and allowed to develop relatively unfettered by regulatory or government policy choices much as the Clinton Administration took a light-touch approach to the development of the Internet in the 1990s.⁸ In order to make those choices, however,

<https://uploads.strikinglycdn.com/files/90847694-70f0-4668-ba7f-dd0c6b0b00a1/RootstockWhitePaper-v9-Overview.pdf>

⁵ Muneeb Ali, Jude Nelson, Ryan Shea and Michael J. Freedman, *Blockstack: A Global Naming and Storage System Secured by Blockchains* (June 2016) <https://blockstack.org/blockstack.pdf>

⁶ Vitalik Buterin, *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform* (Jan. 2014) <https://github.com/ethereum/wiki/wiki/White-Paper>

⁷ Richard Gendal Brown, James Carlyle, Ian Grigg, Mike Hearn, *Corda: An Introduction* (Aug. 2016) <https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/57bda2fdebdbd1acc9c0309b2/1472045822585/corda-introductory-whitepaper-final.pdf>

⁸ President William J. Clinton, Vice President Albert Gore, Jr. *A Framework For Global Electronic Commerce* (July 1997) available at <https://www.w3.org/TR/NOTE-framework-970706#AnnotatedVersion> (“Governments can have a profound effect on the growth of commerce on the Internet. By their actions, they can facilitate electronic trade or inhibit it. Knowing when to act and -- at least as important -- when not to act, will be crucial to the development of electronic commerce.5 This report articulates the Administration's vision for the emergence of the GII as a vibrant global marketplace by suggesting a set of principles, presenting a series of policies, and establishing a road map for international discussions and agreements to facilitate the growth of commerce on the Internet.”)

policymakers need a basic understanding of how consensus works and what it might help us build.

C. Platforms for Innovation: Public or Private

A fundamental question in the design of any consensus mechanism is who can participate and how do they participate in order to reach consensus over some shared computation. For many years it was assumed that useful consensus mechanisms could only be developed if the participant computers were identified through channels outside of the decentralized computing system itself.⁹ In other words, it had been assumed that useful consensus mechanisms could only be designed as private or permissioned systems: to participate in the decentralized computing system a user would need to either (a) gain physical access to a private underlying network architecture (e.g., an “intranet” rather than the Internet) or (b) obtain an access credential via a cryptographic key exchange with other participants or by utilizing a public key infrastructure.¹⁰ Several such private consensus mechanisms have been, and are continuing to be, developed.¹¹

Private consensus mechanisms, however, may not be optimal for the development of robust

⁹ See Jonathan Katz, Andrew Miller, and Elaine Shi, “Pseudonymous Broadcast and Secure Computation from Cryptographic Puzzles” (Oct 2014) *available at* <http://eprint.iacr.org/2014/857.pdf> (“Standard models of distributed computing assume authenticated point-to point channels between parties, where authentication may be provided via some physical property of the underlying network or using keys shared by the parties in advance. When security against a large fraction of corruptions is desired, even stronger pre-existing setup—e.g., a broadcast channel or a public-key infrastructure (PKI) with which broadcast can be implemented—is often assumed. Such setup may not exist in many interesting scenarios, especially open, peer-to-peer networks in which parties do not necessarily have any prior relationships, and can come and go as they please. Nevertheless, such setup is often assumed due to the prevailing belief that nothing “interesting” can be achieved without them, and in fact there are known impossibility results to this effect.”). See also Boaz Barak, Ran Canetti, Yehuda Lindell, Rafael Pass, and Tal Rabin. “Secure computation without authentication.” *Advances in Cryptology—CRYPTO 2005*, pp. 361–377 (2005).

¹⁰ *Id.*

¹¹ See, e.g., Paxos, a widely used protocol for generating consensus across a set of unreliable processors. Marshall Pease, Robert Shostak, and Leslie Lamport, “Reaching Agreement in the Presence of Faults,” 27 *Journal of the Association for Computing Machinery* 228–234 (April 1980). We will not discuss Paxos or related consensus mechanisms within this paper. These systems are generally fault tolerant only under an assumption that none of the nodes are actively attempting to undermine the consensus by sending malicious and deceptive data to other nodes. The ability to deliver a useful distributed computing service despite the presence of malicious and deceptive participants is known in computer science as “byzantine fault tolerance” or BFT. See Kevin Driscoll, Brendan Hall, et al, “Byzantine Fault Tolerance, from Theory to Reality” 2788 *Lecture Notes in Computer Science* 235 (2003). There are BFT variants of Paxos, however, they do not scale effectively to large, highly distributed computing networks. See Marko Vukolic, “The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication,” *IBM Research* (“This is true even for their crash-tolerant counterparts, i.e., replication protocols such as Paxos, Zab and Raft, which are used in many large scale systems but practically never across more than a handful of replicas.”). Accordingly, Paxos is a useful tool for generating an agreement amongst several computers all under one individual or institution’s control. The technologies discussed in this paper are limited to newer mechanisms, inspired by Bitcoin, that seek explicitly to generate agreement amongst a large number of computers controlled by mutually distrustful strangers.

general purpose decentralized computing systems. Access to dedicated network infrastructure and/or public key infrastructure is costly, potentially limiting participation to larger players like businesses. In some cases, these prerequisites are irreconcilable with the desired decentralized computing use case, as when consensus is sought across a peer-to-peer network that allows peers free entry and exit.¹² If, as described in the previous section, we believe that some decentralized computing systems should be public platforms for democratic and diverse innovation (as were the PC and the Internet), then a permissioned system seems like a poor choice.

Private systems may be the smarter choice for limited rather than general purpose decentralized computing tasks, where consensus need not be open to all potential participants and participants can be centrally identified and trusted not to collude against the interests of the group (e.g., when a consortium of banks wants to settle inter-bank loans according to a decentralized ledger).¹³ Permissionless systems are arguably more difficult to scale,¹⁴ to make private,¹⁵ or to secure than private systems.¹⁶ These, however, are technical challenges that may prove to be fully surmountable.

Much of the current skepticism exhibited by proponents of simpler, private systems could prove shortsighted. Similar issues of scale and usability clouded early predictions about computing generally. For example, in 1951 Cambridge mathematician Douglas Hartree suggested that “all the calculations that would ever be needed in [the UK] could be done on three digital computers—one in Cambridge, one in Teddington, and one in Manchester. No one else would ever need machines of their own, or would be able to afford to buy them.”¹⁷ Similar skepticism stalked the early Internet. For example, in 1998 economist Paul Krugman wrote,

The growth of the Internet will slow drastically, as the flaw in “Metcalfe's law”—which states that the number of potential connections in a network is proportional to the square of the number of participants—becomes apparent: most people have nothing to

¹² Katz, *supra* note 9.

¹³ See, e.g., Gendal Brown, *supra* note 7.

¹⁴ See Vukolic, *supra* note 11. See also Kyle Torpey, “Bitcoin Reaches a Crossroads With the Scaling Debate, Not a Crisis” *Bitcoin Magazine* (May 2016) <https://bitcoinmagazine.com/articles/bitcoin-reaches-a-crossroads-with-the-scaling-debate-not-a-crisis-1462980183>.

¹⁵ See *infra* p. 35.

¹⁶ See Robert Sams, “No, Bitcoin is not the future of securities settlement,” (2015) <http://www.clearmatics.com/2015/05/no-bitcoin-is-not-the-future-of-securities-settlement> (“If you are prepared to use trusted third parties for authentication of the counterparts to a transaction, I can see no compelling reason for not also requiring identity authentication of the transaction validators as well. By doing that, you can ditch the gross inefficiencies of proof-of-work and use a consensus algorithm of the one-node-one-vote variety instead that is ... thousands of times more efficient.”).

¹⁷ Lord Bowden, 58 *American Scientist* 43 (1970). This accurate quotation is generally considered to be the basis for a notorious misquote of IBM President Thomas J Watson, “I think there is a world market for maybe five computers.” Brader, Mark (July 10, 1985). “Only 3 computers will be needed...” (Forum post). https://groups.google.com/forum/#!msg/net.misc/390t08t_SZY/d2uJwCwcyQAJ.

say to each other! By 2005 or so, it will become clear that the Internet's impact on the economy has been no greater than the fax machine's.¹⁸

The development of the Internet defied many such skeptics. Before we discuss exactly how public and private consensus mechanisms work, it's important to understand how the internet was and is itself *public*, and how that publicness proved essential to its success.

D. The Internet and Permission

The Internet is revolutionary in large part because it avoids the costs of permissioning described above. The underlying protocols that power the Internet—TCP/IP (the Transmission Control Protocol and the Internet Protocol)—are open technical specifications.¹⁹ Think of them like human languages; anyone is free to learn them, and if you learn a language well you can write anything in that language and share it: books, magazines, movie scripts, political speeches, and more. Importantly, you never need to seek permission from the *Institut Français* or the *Agenzia Italiana* to build these higher level creations on top of the lower level languages. Indeed, no one can stop you from learning and using a language.

When Tim Berners Lee had the idea of sending virtual pages filled with styled text, images, and interactive links over TCP/IP (*i.e.* when he invented the Word Wide Web),²⁰ there was no central authority he needed to approve the project. He could write the standards and protocols for displaying websites—the higher level internet protocol known as HTTP (the HyperText Transfer Protocol), and anyone with a TCP/IP capable server or client could run freely available HTTP-based software (web-browsers and web-servers) to read or publish these new rich web pages.²¹ As a result, the Internet went from a primarily command-line text-only interface to a virtual magazine full of pleasantly styled pages full of text, pictures, and links to other related pages, and it made the transition without any formal body approving the change. Every Internet user was free to opt in or opt out of the new format, the World Wide Web, as they so desired simply by choosing whether or not to read and write internet data with the new higher level protocol, HTTP.

Today, thanks to the public, permissionless architecture of TCP/IP and higher level protocols built on top of it, no one needs to gain access to a private network in order to create a blog or send an email. Nor must an Internet user obtain a certificate of identity to participate in online discussions. Nor must a hardware designer obtain permission to build a new gadget that

¹⁸ Megan Mcardle, “Predictions are Hard Especially About the Future” *The Atlantic* (Dec. 2010) <http://www.theatlantic.com/business/archive/2010/12/predictions-are-hard-especially-about-the-future/68471/>.

¹⁹ Lydia Parziale, *et al.*, *TCP/IP Tutorial and Technical Overview* (Dec. 2006) available at <https://www.redbooks.ibm.com/redbooks/pdfs/gg243376.pdf>.

²⁰ World Wide Web Foundation, *History of the Web*, <http://webfoundation.org/about/vision/history-of-the-web/> last accessed Dec. 2016 (“Had the technology been proprietary, and in my total control, it would probably not have taken off. You can’t propose that something be a universal space and at the same time keep control of it.”).

²¹ *Id.*

can send and receive data from the Internet.²² This publicness has been a major factor in democratizing communications, and spurring vibrant competition and innovation. Anyone can design, build, and utilize hardware or software that will automatically connect to the Internet without seeking permission from a network gatekeeper, a national government, or a competitor.

It is true that businesses often utilize public key infrastructure online, and that this does add a layer of permissioning to the web. When you visit an online bank, for example, your web browser will look for a signed certificate issued by a *certificate authority* that has vouched for the bank's online identity.²³ This begins a process between your browser and the bank that will ultimately encrypt all of your communications while you are navigating the website. This process is known as TLS/SSL (Transport Layer Security and its predecessor, Secure Sockets Layer), and it is the system behind the little green lock consumers are told to watch out for when visiting sensitive websites like banks.²⁴

TLS/SSL, however, is another application-layer Internet protocol—like HTTP—that runs *on top* of the public TCP/IP network. Again, the underlying protocols are the reason for the Internet's publicness. When a consumer device is connected to the Internet these protocols do not ask for identification, certificates, or authentication; they simply assign the new device a seemingly random but unique pseudonym (called an IP Address) in order to have a consistent address for routing data.²⁵ The identified and permissioned layer, TLS/SSL, is running on top of the public and pseudonymous layer.

The layered design of the Internet is not accidental. It is modular, with a public lower layer, in order to enable flexibility. One can always build identified and permissioned layers on top of a permissionless system—as TLS/SSL (a private, identified layer) is built on top of TCP/IP (a public, pseudonymous layer). The reverse is not possible, however. Had the Internet originally been architected to be permissioned and identified, it would have imposed costs and limitations on public participation, and it would have ossified the possible range and diversity of future higher level protocols for identity and permission. When lower layers are permissionless and pseudonymous, on the other hand, the costs of participating are low (merely the cost of hardware and free Internet-protocol-ready software), and such an open platform enables a variety of private or identified higher level layers to emerge and compete for particular use cases where identity and permissioning are essential. For example, PGP and the Web of Trust compete with TLS/SSL as methods for enabling secure and identified

²² *Id.* See also W3C, *Web of Devices* <https://www.w3.org/standards/webofdevices/> last accessed Dec. 2016. (“W3C is focusing on technologies to enable Web access anywhere, anytime, using any device. This includes Web access from mobile phones and other mobile devices as well as use of Web technology in consumer electronics, printers, interactive television, and even automobiles.”).

²³ Microsoft, *What is TLS/SSL?* (Mar. 2003) [https://technet.microsoft.com/en-us/library/cc784450\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc784450(v=ws.10).aspx).

²⁴ Google, *Check Chrome's connection to a site* <https://support.google.com/chrome/answer/95617?hl=en> last accessed Dec. 2016.

²⁵ See Stephanie Crawford, “What is an IP address?” *How Stuff Works* <http://computer.howstuffworks.com/internet/basics/question549.htm> last accessed Dec. 2016.

communications built on top of TCP/IP.

We are still in the very early days of decentralized computing systems, and there remains much uncertainty over which protocols and systems will come to dominate the space. Given that uncertainty, it is possible that these systems will not follow the evolution of the Internet or the PC and instead be permissioned by default at the lower level. The key takeaway from a policy perspective, however, should be (1) awareness of the technological features that enabled the Internet to flourish as a democratic and innovative medium—modularity, publicness, and pseudonymity; and (2) a willingness to allow these new decentralized computing systems to evolve similarly unencumbered even when publicness and pseudonymity cause regulatory confusion or concern because of their newness and sharp contrast with legacy systems.

II. Making Sense of Consensus

It's easy to be excited about the *applications* that can be built on top of decentralized computing platforms. They usually have an easy and provocative elevator pitch: *this app will let you send money instantly*, and *this app will save you from creating and remembering hundreds of passwords!* Talking about the infrastructure that powers and enables those apps, however, is harder because the discussion will often be laden with technical jargon and the purpose of the system will be more abstract (*i.e.*, to create a platform for applications that have human-facing purposes).

These underlying architectures, however, have real ramifications for consumer protection and freedom of choice, so it's important that policymakers and concerned citizens understand the various models that are being developed. Just as it can be daunting to learn about internal combustion or gene sequencing, we understand that knowledge of these topics is key to forming good policy for car safety or GMO foods. Similarly, policy aimed at regulating the application level of decentralized computing (*e.g.*, money transmission, identity provision, consumer device privacy) should be informed by knowledge of the underlying infrastructures. This section will explain those technologies in general, but first a disclaimer:

This is not a document intended for technologists, and many of the salient features of these mechanisms will be spoken of in the abstract. Just as one can explain the principles behind internal combustion engines without discussing the acceptable tolerances in the machining of a piston and gudgeon pin, we will attempt to give an accurate general description of decentralized consensus while avoiding discussion of the merits of sharding or SHA-256.

Speaking generally, the goal of a consensus mechanism is to help several networked participant computers come to an agreement over **(1) *some set of data*, (2) *modifications to or computations with that data*, and (3) *the rules that govern that data storage and computation*.**

To use Bitcoin as an example, the network of Bitcoin users run software with an in-built consensus mechanism. This consensus mechanism helps all of the peers on the network

(Bitcoin users):

1. ***Store agreed-upon data:*** every peer gets a copy of the full ledger of all bitcoin transactions in the history of the network.
2. ***Compute and transform that data:*** recipients of bitcoin transactions can write new transactions thus adding to the ledger all transactions.
3. ***Agree on rules for how storage and computation of that data can take place:*** the ledger is continually updated because all peers listen for and relay new transactions if they are valid, and a lottery is used to periodically pick a random peer to state the authoritative order of valid transactions for chunks of time that are about 10 minutes long. (There are other rules but these are probably the most general and fundamental Bitcoin consensus rules).

If this example is not entirely clear, that's OK. We will expand upon it later in this testimony. The key thing to remember is that *consensus* means that a network of peers can agree upon three things: **(1) data, (2) computation (transformation of the data), and (3) the rules for how computation can take place.**

Any particular *consensus* mechanism can be designed to leverage two techniques in order to ensure agreement over a computation and the associated data.

First, there are what we can call ***automatic rules***. To use an automatic rule, all parties to the consensus can run software on their computers that automatically rejects certain "invalid" computational operations or outcomes on sight. To make a legal analogy, we can think of this as *res ipsa loquitur* (the principle that the mere occurrence of an accident implies negligence), or a rule of strict liability.

For example, Bitcoin's core software defines certain outcomes as always impermissible on sight. Most notably, transactions from one user to another cannot send any bitcoins that have not previously been sent to the sender.²⁶ More simply: I can't hand you cash that hasn't previously been given to me. To be compatible with the larger Bitcoin network, the software you run on your computer *must follow this rule*. If it does not, other nodes on the network will ignore any invalid messages you send using it. You can try to send the network messages that attempt such counterfeiting, but your messages will always fall on deaf ears and the effort will be futile. These are automatic rules that help the network ignore data that is irrelevant or malevolent to the agreement the participants are seeking.

Second, there are what we can call ***decision rules***. In situations where there are two differing outcomes from the computation, but where both would be valid based on the automatic rules, a rule of decision between each possible valid state is needed in order to keep the network in agreement. All parties to the consensus can agree in advance (by choosing which software to run) to always honor one possible valid outcome over another possible valid outcome based on a decision rule. From a legal perspective this is more like a judgement of fact from a jury at

²⁶ Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (Nov. 2008) p. 2
<https://bitcoin.org/bitcoin.pdf>.

trial.

For example, Bitcoin's core software does not tell you when any particular valid transaction comes before another valid transaction in the order-keeping ledger of all historical transactions. This order is, nonetheless, critical to determine who paid whom first. Instead of using an automatic rule to settle uncertainties regarding transaction order, Bitcoin's software specifies a decision rule to resolve debates over which valid transaction came first.²⁷ Specifically, the Bitcoin software calls for a *repeated leader election by proof-of-work*, which we will discuss in a moment while outlining proof-of-work consensus. For now, it's important to simply understand that there are various ways of establishing a decision rule in order to reach consensus over the authoritative state of a decentralized computing system when multiple valid states are possible. All currently employed methods fall into four broad categories: (A) proof-of-work, (B) proof-of-stake, (C) consortium consensus, and (D) social consensus.

A. Proof-of-Work

As just mentioned, Bitcoin employs a *proof-of-work leader election* as the decision rule for determining the order of valid transactions in the blockchain. Such a consensus method might be useful for various decentralized computing systems, but Bitcoin allows us to describe a working example. *Leader election* means that one participant's record of which transactions came first, second, third, *etc.*, will be selected by all other network participants as the authoritative order of transactions for some designated period of time (beginning with that participant's successful election as leader and ending with the next leader election). We can see how this is a rule of decision, it says essentially: *whenever there is disagreement over two alternative but valid outcomes, defer to the chosen leader's choice for the given period.*

Proof-of-work is the specific method found in the Bitcoin protocol that describes how a leader is periodically chosen.²⁸ The proof-of-work system is essential to keeping the consensus mechanism *public*. This "election" is, therefore, not anything like the democratic political process to which we are accustomed. After all, if users come and go, freely connecting to the public network without identifying themselves, how would we ever keep track of who is who, or who is trustworthy and deserves our vote? So instead of having a vote, the network holds a lottery where there will be a random drawing and a winner every so often (roughly every 10 minutes for Bitcoin and every 12 seconds for Ethereum).²⁹

The term *leader election* is the correct computer science term for this architecture,³⁰ but for the

²⁷ *Id.* at 2-3.

²⁸ See Nakamoto *supra* note 26 at 3 ("The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs").

²⁹ See Vitalik Buterin, "Toward a 12-second Block Time" *Ethereum Blog* (July 2014) <https://blog.ethereum.org/2014/07/11/toward-a-12-second-block-time/>.

³⁰ See Indranil Gupta, Robbert van Renesse, and Kenneth P. Birman, "A Probabilistically Correct Leader Election Protocol for Large Groups," *Technical Report, Cornell University* (April 2000) ("The classical specification of the leader election problem for a process group states that at the termination of the

rest of us that sounds like something that involves voting and majorities rather than probabilities and lotteries. For clarity we will use the term *leader lottery* from here onwards.

Selecting a periodic leader via lottery in the real world would be easier than finding one on a peer-to-peer network. We could all meet in a room, introduce ourselves, and make it real simple by having everyone put their names in a hat and have one blindfolded person pull out a winner.

That simplicity doesn't work online. If all our peers on the network are putting names in a digital hat, we have no idea if each digital name matches one-to-one with a real person.³¹ We could reasonably expect some less-than-scrupulous individuals to make up a bunch of random fake names and stick them in the hat. In the digital world we'd have no way of knowing whether Alice, Beth, Chuck, Dana, and Eve are each real individuals or merely pseudonyms (*i.e.*, "sock puppets") made up by Alice in order to have a better chance at winning the lottery. We could try to employ some digital identity system to stop that fraud, but then we would be relying on an external identifier to guarantee the fairness of the system, and that defeats the point of having a public, ungated system to begin with. It would make it costly to participate because you would need to get identified in the real world to do your computing on the decentralized network, and it would force everyone to place trust in the identifier.

Rather than identify all lottery participants and pick names from a hat, we could have a ticket-based lottery, like Powerball. These lotteries only work if the lottery tickets have a cost (if they were free how many tickets to the Powerball would you claim for yourself?). A proof-of-work consensus system merely seeks to make it costly to enter yourself in the lottery. So Alice could still have more than one chance to win, but she incurs real costs every time she buys a new chance.

This has two desirable consequences that help make the lottery a good tool for selecting periodic leaders in a consensus mechanism. (1) *Decentralization*: It would be prohibitively costly to amass enough tickets to ensure that you would be the periodic leader for many repeated periods. (2) *Skin-in-the-game*: Leaders tend to be participants who have made sizable investments in the system by buying costly tickets. Generally speaking, the first reduces the capacity for self-dealing (always putting your transactions first), and the second ensures that the costs of malfeasance are internalized by the participants (who have invested real capital in the long-term success of the platform).

But how do we make those tickets costly when there is no central authority to verify payment? A proof-of-work consensus mechanism imposes costs on participants by making every ticket costly as measured in computing power that provably performs some "work," hence the name proof-of-work. Effectively, every lottery ticket costs one attempt at solving a difficult math

protocol, exactly one non-faulty group member is elected as the leader, and every other non-faulty member in the group knows about this choice.").

³¹ See Nakamoto *supra* note 26 at 3 ("If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs").

problem that can only be solved with guess-and-check.

Think of the Bitcoin lottery ticket as a Sudoku puzzle. To win you need to solve a math puzzle that is difficult (guessing and checking numbers that make rows and columns sum up correctly), but easy for others to check if you have solved it (just sum up the rows and columns). Participants in the network previously agree (with an automatic rule) that the winner of every periodic leader lottery will be the person who first solves the math problem. Ultimately, finding a solution comes down to a lucky guess, but you can make more guesses faster if you have more powerful computers. Because, like Sudoku, it is easy to check someone else's solution, all participants will discover quickly if someone has cracked it, and they will move on to solving the next problem so they can be the leader in the next period.

You might be wondering... *who is setting these problems up?! How is there not an all-powerful algebra teacher controlling Bitcoin?* There isn't, because Bitcoin uses an *open-ended* problem that is specified using only publicly available information found in the Bitcoin protocol software. To extend our classroom metaphor, imagine that the problem on the blackboard is this: *flip a coin heads up 20 times in a row*—a completely open-ended problem. First, we students all agree the problem on the blackboard is the problem we are all competing to solve (an automatic rule), and then once we get flipping, we can all agree if someone does it. Then, once someone “wins,” that person is the leader, and we can begin flipping coins again to determine the next leader. We never need a teacher or central authority to present the next problem, we just go ahead and compute the same problem. It's difficult to get less metaphorical or more specific than that without discussing cryptographic functions,⁵² something we would like to avoid in this general overview.

What is important to take away from this discussion is that participants enter the lottery by guessing solutions to a publicly posted math problem with their computers, and that more computing power will mean more guesses (more coin flips), which means more chances to win. Because computing power is expensive (both in terms of buying computer hardware, and using electricity to power computing cycles on that hardware) every additional lottery ticket has a cost to the participant.

But if lottery tickets in this leader lottery are costly, then why even participate? After all, the prize for winning would be the right to provide what is effectively a public good: offering an authoritative list of valid transactions on the network for a period of time. This could provide the winner with some benefits (such as ensuring that her own transactions get included in the ledger) but most of the benefits go to the other network participants who get to use a public ledger. So, proof-of-work systems also generally provide a cash reward (in the form of the tokens native to the network) to the holder of a winning ticket, usually called *the mining reward*. This reward can be any fees that were voluntarily appended to transactions by senders on the network (in order to make their transactions more appealing for an elected leader to

⁵² For a non-technical but more comprehensive explanation of how the bitcoin proof-of-work process operates, see Peter Van Valkenburgh, “What is Bitcoin Mining, and Why is it Necessary?” *Coin Center* (Dec. 2014) <https://coincenter.org/entry/what-is-bitcoin-mining-and-why-is-it-necessary>.

include in the section of the ledger she is writing), as well as permission within the software's automatic rules to create new money by sending herself a transaction with no source of funds (socializing the cost of a reward through inflation).³³

Bitcoin users who decide to participate in this leader lottery have come to be called Miners because they perform "work" in return for newly created value. The label, however, belies the larger role these participants play in generating and maintaining consensus across the decentralized computing system. Both the work and the reward are secondary technical features necessary to the creation of a decentralized mechanism for picking periodic leaders who can ensure that data discrepancies between participants are quickly and fairly resolved.

Without a reward baked into the consensus mechanism, it is hard to understand why users would be incentivized to participate honestly in maintaining the network. Much fuss has been made over developing a "blockchain without the bitcoin," as if the currency aspect of the network pollutes what would otherwise be a useful network technology with an ideology or political agenda (or, at the very, least creates too many regulatory complications to be worth the trouble). But, as we can see, the only way to maintain a public network where leaders need to be periodically selected and rewarded for their participation is to award them with tokens that are native to the network itself (*i.e.*, the transaction history and scarcity of the token are a part of the data over which the consensus network is continually coming to an agreement). If participants are rewarded with assets that exist only according to data structures outside the network (*e.g.*, dollars or yen, the balances and scarcity of which are described in the balance sheets of banks) then we've reintroduced the need for identified parties who must be trusted to perform the rewarding function honestly and without bias.

Public blockchain networks need scarce tokens for technical reasons, not (merely) because their proponents may have political or ideological motivations for supporting alternative currencies. Ethereum, for example, is a public consensus-driven decentralized computing network that aspires to provide several user applications aside from electronic cash (*e.g.*, identity management,³⁴ reputation accounting,³⁵ community governance,³⁶ etc.), but it still has

³³ Recall that this is a violation of the automatic rule we discussed earlier in Bitcoin—this is the one exception to that automatic rule, you can send funds without referencing a funding source if and only if you won the leader lottery for the period when you send the transaction; this special transaction is called a coinbase transaction and the amount you are allowed to send is capped according to the monetary policy of the cryptocurrency—yet another automatic rule in the software.

³⁴ See, *e.g.*, Thomson Reuters, *BlockOneID for Ethereum: An identity mapping service for Ethereum blockchains*, <https://blockone.thomsonreuters.com/> last accessed Dec. 2016.

³⁵ See, *e.g.*, Jack Peterson and Joseph Krug, *Augur: a Decentralized, Open-Source Platform for Prediction Markets*, <http://bravenewcoin.com/assets/Whitepapers/Augur-A-Decentralized-Open-Source-Platform-for-Prediction-Markets.pdf>.

³⁶ See Vitalik Buterin, "An Introduction to Futarchy" *Ethereum Blog* (Aug. 2014) <https://blog.ethereum.org/2014/08/21/introduction-futarchy/> ("Although our modern communications technology is drastically augmenting individuals' naturally limited ability to both interact and gather and process information, the governance processes we have today are still dependent on what may now be seen as centralized crutches and arbitrary distinctions such as 'member', 'employee', 'customer' and

a scarce token that rewards winning participants in the leader lottery: ether. A blockchain without bitcoin or similarly scarce token is a private network, essentially a shared database with pre-identified and authenticated users.

To recap, a public consensus method should allow anyone to participate without obtaining some sort of credential from an external identifier. Without identification, however, a user could pretend to be several users and gain an unfair advantage in the leader lottery used to reach agreement when there are disputes over two or more valid outcomes (like alternative orders of transactions in a ledger). To deal with this problem, participation in the leader lottery is made costly by demanding that participants solve difficult math equations that will require costly hardware and electricity—proof-of-work. As a result, it (A) becomes too expensive to dominate the lottery by obtaining a substantial number of tickets, and (B) ensures that lottery winners are invested in the long-term success of the decentralized computing system. Winning participants are, in turn, rewarded with a scarce token native to the network.

B. Proof-of-Stake

Now that we have an intuitive understanding of proof-of-work consensus, it is fairly simple to explain the general mechanism behind proof-of-stake consensus. Recall that the goal behind proof-of-work is to make participation in the consensus costly. If the consensus mechanism involves a leader lottery, then we employ proof-of-work to make buying up all the lottery tickets prohibitively expensive.

Proof-of-stake systems are also designed to make participation come at the cost of some provable sacrifice. Instead of requiring calculation in exchange for a lottery ticket, a proof-of-stake mechanism requires that participants prove that they hold and/or can temporarily forgo access to a valuable token that travels on the network.³⁷ So if Bitcoin was a proof-of-stake-based cryptocurrency, then participation in the lottery could require users to stake some of the bitcoins they control—to prove that they control or to sacrifice their control over those valuable funds. The mechanism could demand that participation requires merely a mathematical proof that the user has possession of these tokens on the blockchain, or it could

‘investor’ – features that were arguably originally necessary because of the inherent difficulties of managing large numbers of people up to this point, but perhaps no longer. Now, it may be possible to create systems that are more fluid and generalized that take advantage of the full power law curve of people’s ability and desire to contribute. There are a number of new governance models that try to take advantage of our new tools to improve transparency and efficiency, including liquid democracy and holacracy; the one that I will discuss and dissect today is futarchy.”).

³⁷ See Vitalik Buterin, “What proof of stake is and why it matters” *Bitcoin Magazine* (Aug 2013) <https://bitcoinmagazine.com/articles/what-proof-of-stake-is-and-why-it-matters-1377531463> (“Rather than requiring the prover to perform a certain amount of computational work, a proof of stake system requires the prover to show ownership of a certain amount of money. The reason why Satoshi could not have done this himself is simple: before 2009, there was no kind of digital property which could securely interact with cryptographic protocols. Paypal and online credit card payments have been around for over ten years, but those systems are centralized, so creating a proof of stake system around them would allow Paypal and credit card providers themselves to cheat it by generating fake transactions.”).

demand the permanent relinquishment or even destruction of these token (something often referred to as “proof-of-burn”³⁸), or it could be a temporary stake, effectively a bond (e.g., I stake 50 bitcoins—and thereby relinquish my ability to spend them—for the next 150 cycles of the leader lottery at which point I will regain control over the coins and can decide whether to stake again in the future). Regardless of how exactly it is specified, the goal is to use the value of the tokens (rather than the cost of computing) as the provable signal necessary for participation in the leader lottery.

If the tokens that travel on this decentralized network are available for sale on a variety of competitive exchanges (whether in exchange for dollars, euros, or other cryptocurrencies) or can be obtained by free transfer from existing users (whether as a gift or in payment for labor or some valuable good) then anyone with sufficient economic resources can, in theory, join the consensus, because they can obtain the tokens necessary to offer a proof-of-stake. In this sense, proof-of-stake consensus methods are, like proof-of-work methods, public.

C. Consortium Consensus

Consortium systems have a simpler solution to making lottery-style elections fair: only allow identified parties to participate. If we decide to trust an outside authority to identify all consortium members, provisioning members with cryptographic keys which they can use to sign their communications and prove authenticity, then we can run software that would only grant lottery tickets to participants who send validly signed messages.³⁹ We know Alice, Beth, Chuck, Dana, and Eve are each real individuals because we previously provisioned them each

³⁸ See Counterparty, “Why Proof-of-Burn” *Counterparty Blog* (Mar. 2014) <http://counterparty.io/news/why-proof-of-burn/>.

³⁹ When all parties are identified and can be trusted we may not even need a provably fair leader lottery; the leader could simply be the consortium participant with the best quality connection to the network, or it could rotate according to a pre-established order, or an upcoming schedule of leaders could be picked by an offline meeting of participants every year. Indeed, the identified parties could simply choose to use one of the many pre-blockchain fault-tolerant consensus protocols, e.g. Paxos, which have a long (around 25 years) and established track record (see Pease *supra* note 11), or perhaps simply a basic distributed database tool, e.g. an Oracle Database product. It is the longstanding availability of these tools and their persistent non-adoption by the financial industry that has spurred many to cynically characterize the present enthusiasm for permissioned blockchains as nothing more than a bitcoin-inspired and blockchain-branded pitch for selling marginally improved infrastructure to conservative institutions. See, e.g., Wences Casares, (Panel Remarks) *Tech Crunch Disrupt: Is it time to stick a fork in Bitcoin?* (Sep. 2015) <https://www.youtube.com/watch?v=ORcFGBhDDis> (“That’s called a private database, and it has existed for a long time. What’s new about Bitcoin is that it’s a decentralized, trustless ledger. The second you do it your own it’s called a private database, and they have existed for a very long time. There’s nothing revolutionary about that. ... If you’re a Visa executive, Bank of America executive, or a Wells Fargo executive, it has become very fashionable to say, ‘I really, really like the blockchain. I’m very interested in the blockchain, but I’m not interested in bitcoin,’ which is the equivalent of saying, ‘I really like the browser, but I don’t like the Internet.’ It’s ridiculous. Those people don’t want to be the ones who didn’t see the Internet coming, and they want to say something nice about it without saying something nice about it. They don’t realize that the blockchain does not work without bitcoin. The blockchain is the first decentralized, trustless database because the miners maintain it, and the miners do so because they get paid in bitcoin. Even though there are a lot of nice use cases on top of that, none of them work without the miners being paid with bitcoin.”)

with secret keys and to obtain a lottery ticket each signs a message with his or her unique key.

This consortium method avoids the costs of solving math problems or staking valuable tokens that is inherent in proof-of-work and proof-of-stake systems.⁴⁰ The consortium method, however, also reintroduces permission and trust into the decentralized computing system. We need to be identified and granted access to the network in order to participate and we need to trust that the party tasked with making these identifications is acting fairly.

D. Social Consensus

Finally, we come to the last general category of consensus mechanisms, social consensus. You can think of the social consensus mechanism as somewhere in between the fully identified and permissioned consortium model, and the fully pseudonymous and public proof-of-work and proof-of-stake models.

Like the consortium model, you choose to trust some identified participants rather than relying on pseudonymous participants who offer a costly signal of credibility. Unlike the consortium model, however, each individual is her own identifying authority; she can choose which counterparties she trusts and build a social network of those with whom she feels comfortable entrusting the role of writing new data to the blockchain (or agreeing on some computation generally). We might then expect various users with differing social networks to disagree over the authoritative state of the consensus data, but the network can be designed to come to global agreement by looking for a subset of all transaction or computation data that some minimum number of trusted participants (perhaps a majority or a supermajority of trusted participants on the network) have agreed upon.⁴¹

As with proof-of-work and proof-of-stake consensus mechanisms, a social consensus mechanism will generally be public. Anyone can join but they must be selected as trustworthy by some minimum number of participants before they can participate in full.

III. Publicness, Trust, and Privacy Across Various Consensus Models

We've spent a good deal of time outlining these various consensus models because the specifics of their architecture will inevitably have meaningful consequences for the applications that are built on top of them, and, by extension, the people who will use those applications. One does not simply procure some "blockchain technology" to build better digital identity systems, property registries, voting infrastructure, or any of the other ambitious killer apps that have been proposed and widely touted for this technology. Building

⁴⁰ See Sams *supra* note 16.

⁴¹ See, e.g., the Ripple Protocol's consensus mechanism. David Schwartz, Noah Youngs, Arthur Britto, *The Ripple Protocol Consensus Algorithm* (2014) <https://ripple.com/consensus-whitepaper/> ("Each server, maintains a unique node list (UNL), which is a set of other servers that s queries when determining consensus. Only the votes of the other members of the UNL of s are considered when determining consensus (as opposed to every node on the network). Thus the UNL represents a subset of the network which when taken collectively, is "trusted" by s to not collude in an attempt to defraud the network.").

any of those applications will require either (A) the modification and use of an existing consensus network (e.g., build the application on top of Bitcoin or Ethereum) or (B) the creation of a new consensus network (both the development of consensus software and the bootstrapping of a network of peers who run the software that generates the consensus). The choice of whether to use one of the existing *public* (i.e., proof-of-work, proof-of-stake, or social consensus) networks, to create a new *public* network, or to design and implement a private consensus network will be a choice that affects the relative publicness of the application, the degree of trust that users must place in other users or maintainers of the application or the underlying network, and the degree of privacy that the application is capable of offering its users. Each of these key consensus mechanism attributes, publicness, trust, and privacy will now be discussed in turn.

A. Publicness Across Consensus Mechanisms

Speaking generally, public consensus-driven decentralized computing systems are exciting and disruptive because their publicness resembles the early Internet. As we described previously, the Internet became the vibrant ecosystem we know today largely because it is so easy to build hardware or software that can seamlessly integrate with TCP/IP, the lower level networking protocol (language) that powers the network. That lower level is pseudonymous. Devices connect to the network and are automatically assigned a seemingly random number rather than a real-world identity.⁴² The lower level is permissionless. Devices can send or receive data to and from any other pseudonym so long as the messages conform to the protocol specification.⁴³ The lower level is general purpose and extensible. TCP/IP only describes how packets of data should move through the network. It does not dictate what the contents of those packets can or should be.⁴⁴ Higher level protocols can be built on top of TCP/IP to interpret sent data as web pages, links, videos, emails, SWIFT bank messages,⁴⁵ anything that can be imagined, invented, and digitized.

The similarity of TCP/IP to Bitcoin, Ethereum, or any other public blockchain network should be apparent. These systems are also pseudonymous. Users are assigned random but unique cryptographic addresses.⁴⁶ These systems are also permissionless. Users can read or write data to the blockchain at will, sending or receiving transactions without seeking the permission of any centralized party. And these systems are also general purpose and extensible. Several parties are building new applications and application layers on top of the Bitcoin network,⁴⁷

⁴² Crawford *supra* note 25.

⁴³ W3C *supra* note 21.

⁴⁴ *Id.*

⁴⁵ Starting in the late 90s several standardized bank messaging services and cooperatives transitioned or adapted their systems to utilize TCP/IP as an underlying networking protocol. SWIFT messages travel over SWIFTNet a higher level Internet protocol that runs on top of TCP/IP. Additionally, the network that supports Fedwire messages, FEDNET, and CHIPS (the international Clearing House Interbank Payment System) network are both built to run on top of TCP/IP. See Roy S. Freedman, *Introduction to Financial Technology* (Apr. 2006) pp. 241-246.

⁴⁶ Here is an example of a bitcoin address: 1CPwNAct62wts2yGb1vUuqeGD58SszeAL.

⁴⁷ See, e.g., Lerner *supra* note 4, and Ali *supra* note 5.

and Ethereum is explicitly designed to be a flexible foundation for building any trust-minimized application.⁴⁸

In the previous section we classified four types of consensus mechanism into two groups:

- **Public:** Proof-of-work, Proof-of-stake, Social Consensus
- **Private:** Consortium Consensus

Decentralized computing systems built using public consensus mechanisms will, in general, be available to any participants who have an internet-connected device and free software that is compatible with the network. Systems built using a private consensus mechanism will, in general, only be available to participants who have previously identified themselves offline and been granted some form of credential by the identifying authority, which they can use to authenticate their identity whenever they connect to the network.

This characterization of publicness lacks, however, an important nuance. There are basically only two things that any user or potential user might want to do with a decentralized computing network: (1) write data to the network and have it included in the consensus-derived data structure or blockchain, or (2) read data from that network's consensus-derived data structure. Accordingly, a Bitcoin user making a transaction is *writing* new data to the Bitcoin blockchain while a user who queries their balance to confirm payment receipt is *reading* data from the blockchain.

Some have characterized networks where users can freely write consensus data as “permissionless.” That is in contrast to “permissioned” networks where users need off-network identification and authentication in order to write. Read access is then characterized as public (anyone can read consensus data) vs. private (only identified and authenticated participants can read consensus data). These terms, however, can be confusing (is a network that has public read-access but private write-access truly public?) so we will continue to use public only in cases where both reading and writing are open to general participation and private in all other cases. For clarity we can summarize this more nuanced characterization with a four-by-four matrix:

⁴⁸ See Buterin *supra* note 6.

		Writing Data Requires:	
		Internet-connected device, free software, and proof-of-work or proof-of-stake.	Off-network Identification, Authentication, and Permission.
Reading Data Requires:	Internet-connected device and free software.	Public (Permissionless, Public Blockchain)	Public for Reading, Private for Writing (Permissioned, Public Blockchain)
	Off-network Identification, Authentication, and Permission.	Public for Writing, Private for Reading (Permissionless, Private Blockchain)	Private (Permissioned, Private Blockchain)

Note an important subtlety in this chart. Public for reading is characterized as requiring only that the reader have an Internet-connected device and free software, while public for writing requires those things but also a proof, either of work or of stake. Bitcoin and Ethereum both exhibit this form of read/write publicness. Anyone with an Internet-connected device and free software can connect to these networks and download the full set of consensus data, *e.g.* the blockchain or list of all valid transactions made on the network from its start. Writing new data to these networks is not quite as easy. If one wants to truly be the node on the network that adds new data to the blockchain, one will have to be selected in the leader elections described in the previous section.⁴⁹ So, to truly write new data on these networks one must provide a proof (of computer work or of stake in the network's native token) and then be selected in the network's leader lottery. Even then, however, the user will only truly *write* data to the blockchain for those periods in which she has been chosen as leader.

This, however, is an overly pedantic description of who may write data on these networks. Thousands of people *do* write data to these public blockchain networks without ever running a node that makes a proof, *i.e.* mining. This is because anyone can send a new transaction message to various peers on the network and reasonably expect that the transaction will be picked up by a proof-making node, *i.e.* a miner, who will then incorporate it into a block of transactions which will then be added to the blockchain when that miner wins the leader lottery for a given period. Non-mining peers who want to ensure that their transaction will be written to the blockchain quickly can attach a fee to that transaction which will reward the

⁴⁹ See *infra* at 17.

miner who wins the leader lottery and is the first to incorporate the transaction in the blockchain.⁵⁰

Relying on these proof-making nodes to write data may seem like a kind of permissioning, and it is true that any particular user who is chosen in the leader lottery can, for that period, decide which new data will and which new data will not be written to the blockchain. Taking Bitcoin for example, it is true that for the duration that a miner wins the leader lottery, she can censor or block any other user from transacting.

There are two factors that make these systems permissionless in spite of the power of miners or proof makers to block or screen write-access: self-interest among competing proof makers, and ignorance of the data that enters the blockchain.

Self-interest. If a user wants to ensure that her transaction will be added to a public blockchain, she can append a fee to the transaction.⁵¹ Miners or proof makers on the network compete with each other for the block rewards that come with winning the leader lottery. Block rewards are comprised of any fees that were appended to transactions as well as any new money being created through programmed inflation. It is with these block rewards that miners can finance the expensive hardware and electricity necessary to perform competitive proof-of-work calculations or justify the costly sacrifice of tokens necessary in making a proof of stake. Blocking transactions will reduce the fee-revenue component of the block reward, leaving censorship-favoring proof makers at a competitive disadvantage. Therefore it goes against the self-interest of proof makers to selectively censor (*i.e.*, permission) the network. Additionally, to the extent that a network is famed for being censorship resistant, *e.g.* Bitcoin,⁵² negative publicity from a proof maker's decision to censor transactions may erode faith in the network as a whole. This could cause the market price of the network's tokens to fall, thereby reducing the real value of the proof maker's returns and/or motivating the community to enforce anti-censorship norms by shaming the offending proof maker.

Ignorance. Proof makers may not have very much information about the data they are writing to the chain. In other words, the proof maker may know that a particular transaction is valid (because the digital signatures are valid and the sending address is appropriately funded) but she may have no way of knowing who the real-world sender or recipient in the transaction could be. As we will discuss in the section on privacy,⁵³ new technologies such as zero-knowledge proofs, could ensure that proof-makers as well as the public can gain effectively no information from the blockchain aside from a proof that all transactions are valid according to the consensus rules of the protocol. In this situation, proof-making or mining become an activity divorced from any sort of off-network or personal decision making,

⁵⁰ See Nakamoto *supra* note 25.

⁵¹ *Id.*

⁵² See, *e.g.*, Rainey Reitman, "Bitcoin – a Step Toward Censorship-Resistant Digital Currency" *EFF Deeplinks Blog* (Jan. 2011) <https://www.eff.org/deeplinks/2011/01/bitcoin-step-toward-censorship-resistant>.

⁵³ See *infra* at 35.

people simply run machines that always add data to the blockchain if it is valid according to the rules of the protocol and are never in a position to discriminate against users for any other reason.

It's simply not necessary to go into this highly nuanced analysis when it comes to consortium-based consensus mechanisms. By definition, these systems will be permissioned at the write-level because only previously identified participants can participate in the consensus. A choice could then be made by the designers of the system, to make read-access to the results of that consensus public or private.

B. Trust Across Consensus Mechanisms

Early decentralized computing systems, like Bitcoin, are designed for serious uses. These networks custody people's valuables, help them move their money.⁵⁴ These networks may soon keep track of their users' identity credentials,⁵⁵ and eventually even—in the case of the Internet of Things—help them control their door locks, their baby monitors, their cars, and their homes.⁵⁶

A fundamental design goal of these systems is to decentralize control over the network such that a user will not need to trust a bank-like company's honesty in order to safeguard her money,⁵⁷ or trust a technology company in order to safeguard access to her smart home devices.⁵⁸ Who or what do you trust to guarantee these systems if not a reputable intermediary, and how does that model of trust change depending on the type of consensus mechanism employed in the system's design? These are the questions addressed in this subsection.

To start, any discussion of trust must deal with three essential subtopics:

- **Software:** Every system described in this testimony is built from software, and the auditability of that software, as well as the nature of the process of writing that software is the first concern we should have when we ask ourselves: can I trust this system?

⁵⁴ See *infra* at 45. See also Nakamoto *supra* note 26.

⁵⁵ See *infra* at 51. See also Ali *supra* note 5.

⁵⁶ See *infra* at 58. See also Peter Saint-Andre, "How can blockchains improve the Internet of Things?" *Coin Center* (Oct. 2016)

<https://coincenter.org/entry/how-can-blockchains-improve-the-internet-of-things>.

⁵⁷ See Nakamoto *supra* note 26 ("What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.").

⁵⁸ See IBM Institute for Business Value, *Device Democracy: Saving the future of the Internet of Things*, <https://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03620usen/GBE03620USEN.PDF> ("The Internet was originally built on trust. In the post-Snowden era, it is evident that trust in the Internet is over. The notion of IoT solutions built as centralized systems with trusted partners is now something of a fantasy. Most solutions today provide the ability for centralized authorities, whether governments, manufacturers or service providers to gain unauthorized access to and control devices by collecting and analyzing user data.").

- **Consensus:** The software describes what we have called automatic rules and decision rules. The administration of these rules and the creation of consensus amongst the participants of the system is our second concern with respect to trust.
- **Purpose:** “Trust” or “trustworthiness” is not a monolithic whole. The parties to the system may demand varying requirements from the system: a system to operate an office sports betting pool may not need to be as trustworthy as a system for executing interest-rate swaps among banks. Additionally, the parties to the system may have a good reason to put faith in their fellow participants, and therefore they may not need a system designed to fully supplant trust in one’s counterparties.

i. Trust in Software

As a first pass, it is important to recall that much of the agreement between participants in these systems is established by what we called automatic rules that are specified in the software. Additionally, we must remember that decision rules will also always be described in the software, even if the decision-making process is then carried out by network participants (whether through proof-of-work, proof-of-stake, consortium, or social consensus means). The software is therefore, to make another legal analogy, the constitutional law of the network; it describes the process by which all subsidiary legal structures should and will ultimately function. The software is always the first element of the system that we must consider when judging the system’s relative trustworthiness.

As a general rule, open-source software (*i.e.*, software whose source code can be viewed and audited by any and all interested parties free of any need to seek a copyright license or permission from a patent holder) may be preferable in the context of decentralized systems.⁵⁹

⁵⁹ There is a vibrant debate over the relative security of open vs. closed source software in general, and strong arguments on both sides. We take no position in this debate. In the specific context of decentralized networks, however, open source software may have an advantage. In a typical, centralized computer system there will be one entity who, as an individual, business, or institution, is legally accountable to the users of its products and therefore motivated to carefully procure software tools, establish relationships with reputable vendors and/or design software in house, and ultimately audit the tools they chose to implement in their system, whether they be open- or closed-source. In a decentralized system and then agree on which solutions to use. These unaffiliated individuals may not share the same level of trust in a particular vendor of closed-source software. Geographically and culturally diverse, participants may not share the same capabilities for legal recourse against a vendor in the event of negligence, and they may not be able to rely on the vendor for support in the event of a failure that affects them disproportionately to the rest of the network. Popular open-source software projects do not rely on the reputation of a particular vendor to establish trust. Instead, an open community of participants independently develop and audit the code. Open source software is, by definition, publicly available for audit, and would therefore allow the several uncoordinated stakeholders in a decentralized computing system to more easily judge the source code and make decisions for themselves regarding security. Even the developers of *private consensus mechanisms* have felt it prudent to nonetheless make their *software open-source*, likely for this very reason: they need to convince several unaffiliated parties (*e.g.* a consortium of banks) of the software’s fairness and validity, while assuaging fears of vendor lock-in. See, *e.g.*, Jemima Kelly, “Exclusive: Blockchain platform developed by banks to be open-source” *Reuters* (Oct. 2016) <http://www.reuters.com/article/us-banks-blockchain-r3-exclusive-idUSKCN12K17E>.

Open-source practices provide an opportunity for developer transparency, an opportunity for a developer or group of developers to put their cards on the table and show with precision what it is they are building. It also subjects that design to an unbounded set of potential security auditors who may detect innocent mistakes as well as malicious backdoors.⁶⁰ Without visibility into the software we are putting a good deal of faith in the person selling us that software or advocating for its use. Closed-source software, also referred to as proprietary software, may be superior for various applications (e.g., a word processor or a game), but for decentralized applications that we intend to trust with our money, reputation, identity, or any other valuable agreement between users, close-source software creates real risks. To extend our legal metaphor, a closed-source consensus protocol is not unlike a constitution that no one in the country is allowed to read without seeking permission from the drafter or central government.

To give a real-world example, imagine if someone decided to create an alternative to Bitcoin by copying and modifying the Bitcoin software. What if this person changed the automatic rule that requires all transactions to be funded by prior transactions, to a rule stating that one particular pseudonymous participant would be allowed to send transactions out of thin air. If we are going to use this bizarro-Bitcoin as a shared currency, we would certainly want to know that this change to the software's automatic consensus rules has been made. Our new bizarro-Bitcoin network is now allowing one special user to print money to her heart's content. If we have no way to freely read and audit that code (or to rely on a diverse range of third-party validators to do that audit independent of the software author) then we have no reason to trust the network it creates or the agreements it powers.

ii. Trust in the Consensus

After looking at the software, we next need to judge the trustworthiness of the consensus mechanism implemented by the software. Regardless of what some more fervent advocates of these new technologies may say, no system is truly "trustless." No system relies purely on "math" or "cryptography" to ensure that the agreement reached by the network is in any way just or perfect. Instead, these systems are designed to be *trust minimizing*, designed to rely as little as possible on the honesty of the network's participants, usually by making deceptive or fraudulent participation go against the economic interests of the participants. So, aside from being public or private, we can also discuss how each category of consensus mechanism attempts to minimize trust.

In proof-of-work and proof-of-stake systems, so long as we believe that the participants who together control a simple majority of the total computational power on the network (for proof-of-work) or the staked token value on the network (for proof-of-stake) are behaving honestly, then the network's decision rules will work as intended. The need for trust in the

⁶⁰ The idea of security by way of massive public auditing and transparency has come to be called "Linus' Law" and it is commonly expressed as "Many Eyes Make All Bugs Shallow." See Jeff Jones, "Linus's Law aka 'Many Eyes Make All Bugs Shallow'" Microsoft Cyber Trust Blog (Jun. 2006) <https://blogs.microsoft.com/cybertrust/2006/06/07/linuss-law-aka-many-eyes-make-all-bugs-shallow/>.

network's participants is obviated so long as half of its participants are not united in trying to attack it. If a dishonest party or parties assumes control of a simple majority of the computational power or staking ability on the network, then they can effectively control the outcome of all decision rules, and the results may differ substantially from the expectations of honest participants.

To take Bitcoin as an example, a party with majority control of the network's total computational power could: (1) refuse to put certain transactions into the shared ledger indefinitely, (2) consistently favor her own transactions over others in the speed with which they are recorded in the ledger, and (3) periodically rearrange the ledger's order going back as far in history as she has had the majority of power on the network.⁶¹ She cannot, however, violate the automatic rules on the network: she cannot spend other people's bitcoins, nor can she create more bitcoins than would normally be allowed under the monetary policy rules of the software. By sending messages that violate these automatic rules, she loses compatibility with the network and ceases to take part in the consensus mechanism that enforces decision rules like transaction order.

So in proof-of-work and proof-of-stake systems, we can generally trust that the shared computation is valid and fair so long as we believe it is cost-prohibitive for a malicious actor to amass sufficient computing power or staked tokens to have a majority on the network.

Proof-of-stake systems still lack a robust working prototype. The most notable system, Peercoin, suffered a spate of attacks and reverted to a state where the developers created a whitelist of permissible stakers (effectively a consortium model).⁶² Some theorize that a robust proof-of-stake consensus mechanism is an impossible goal, but considering that is beyond the scope of this testimony.⁶³

The availability of what is called "forking"⁶⁴ adds an additional wrinkle to the question of trust

⁶¹ This is commonly referred to as a 51% attack. The limited ability to do harm and exorbitant cost of the attack, combined with the ease with which an attack would be noticed by the community and resolved with modifications to core software lead many to believe that such attacks should be low on the list of threats to the security and trustworthiness of the Bitcoin network. See Gavin Andresen, "Neutralizing a 51% Attack" *GavinTech* (May 2012) <http://gavintech.blogspot.com/2012/05/neutralizing-51-attack.html>; see also Daniel Cawrey, "Are 51% Attacks a Real Threat to Bitcoin?" *Coindesk* (June 2014) <http://www.coindesk.com/51-attacks-real-threat-bitcoin/>.

⁶² Andrew Poelstra, "A Treatise on Altcoins" 14 (Mar. 2015) <https://download.wpsoftware.net/bitcoin/alts.pdf>.

⁶³ For a technical analysis of proof-of-stake systems see Poelstra *supra* note 61 at 14.

⁶⁴ This use of "fork" comes from the larger world of free and public source software development, particularly the communities developing Linux, the open source and oft-forked operating system that powers many enterprise computing systems. Forking refers to a decision amongst some developers within an open source project to duplicate the code of that project and maintain it separately in order to create some derivative invention. See Benjamin Mako Hill, "To Fork or Not To Fork: Lessons From Ubuntu and Debian" (May 2005) https://mako.cc/writing/to_fork_or_not_to_fork.html ("The act of taking the code for a free software project and bifurcating it to create a new project is called 'forking.' There have been a number of famous forks in free software history. One of the most famous was the schism that led to the parallel development of two versions of the Emacs text editor: GNU Emacs and XEmacs.

in networks that utilize public consensus mechanisms. If two or more factions of users on the network fail to reach an agreement over what we have called “automatic rules,” then the network will divide in two or more parts. They will share a computational history up until this impasse but, from the time that one faction chooses to alter their software’s automatic rules onward, they will forge new and distinct futures. This has been the case in several so-called *hard forks* of cryptocurrency networks.⁶⁵

To understand the trust implications of hard forks, we need an example. According to an automatic rule in the Bitcoin consensus mechanism, which we’ll call the *supply rule*, there can only ever be 21 million bitcoins.⁶⁶ This hard limit in the code forms the basis of Bitcoin’s value proposition: you are willing to hold and trade these otherwise made-up tokens for real goods because their supply is known to be finite. With supply fixed, any demand from a community of users will result in a positive price. If we choose to trust Bitcoin’s long-term valuation, we’ll have to worry about fluctuations in demand affecting the price, but at least we won’t need to worry about an increase in supply diluting the value of our holdings with inflation. The effect of the *supply rule* is to Bitcoin’s value as the effect of the earth is to the value of gold when it resists gold-mining.

While it has never happened, we could imagine a fork of Bitcoin where part of the network wants to increase the total supply of bitcoins from 21 to 42 million by changing that automatic rule. We’ll call the more-bitcoins partisans KeynesCoiners, and the rest of the users we’ll call MiltonBitters. As soon as the KeynesCoiners update their software to incorporate a change in the supply rule, transactions and blocks from a KeynesCoin computer are invalid when received by a MiltonBit machine and vice versa. Both sides of the network recognize a common history of bitcoin transactions, but going forward they will have irreconcilable futures. If you

This schism persists to this day.”).

⁶⁵ The most notorious fork in recent crypto-times is probably the hard fork of Ethereum during the DAO hack in the summer of 2016. In response to a bug in a widely funded smart contract (the DAO), developers offered a change to the core protocol that would effectively unwind the result of that contract on the blockchain and make DAO investors whole. A minority of network participants disagreed with this policy and refused to update their software. The result was a fork of the network and the creation of Ethereum Classic (effectively an alternative version of Ethereum). While the drama generated a good deal of press from those critical of Ethereum or simply interested in these networks, it should be noted that the price of Ethereum two months before (April 18th: \$8.44) and two months after the fork (August 18th: \$11.06) shows little evidence for an erosion of trust in the network. For more on the Ethereum fork see Joon Ian Wong and Ian Kar, “Everything you need to know about the ethereum hard fork” *Quartz* (July 2016)

<http://qz.com/730004/everything-you-need-to-know-about-the-ethereum-hard-fork/>.

⁶⁶ There is no line of code in the Bitcoin reference client that specifically says, “there will only ever be 21 Million bitcoins.” Instead, there is language that describes the permissible size of the reward of new bitcoins that miners who mine new blocks can claim in a coinbase transaction. This reward is referred to as a “block subsidy” and it is coded to start at 50 bitcoins per block and decrease by half on a schedule that would result in a final total supply of roughly 21 million total bitcoins at some point in the year 2140. See Bitcoin Core, “main.cpp,” <https://github.com/bitcoin/bitcoin/blob/master/src/main.cpp>, lines 1380-1391 (“Subsidy is cut in half every 210,000 blocks which will occur approximately every 4 years.”). See also “Controlled supply,” Bitcoin Wiki, https://en.bitcoin.it/wiki/Controlled_supply (last accessed Dec. 2015).

held bitcoins before the fork, you now have bitcoin balances on both networks (because they share a common history before the fork), and you can run KeynesCoin software on one computer while running MiltonBit on another in order to move your bitcoins on either or both sides of the newly forked network.

Does this violate the trust that users placed in the supposedly sacred 21 million limit? It's hard to say. The MiltonBit network remains a working cryptocurrency for users who want to stick with the 21 million limit, and pro-inflation revolutionaries can switch to the KeynesCoin chain. In fact, now users who are indifferent as to a choice between 21 and 42 can choose to wait it out, or to use both, because their bitcoin holdings are in the history of both sides of the fork and will remain on each chain unless they decide to transact using the compatible software of that chain. To use a term from political science, forking facilitates political *exit* rather than *voice*, leaving a community with whom you disagree rather than lobbying for a change to that community's rules.

It's not all rosy, however. When our hypothetical network split in two, the supply curve changed for only one-half of the network but the demand curve for each coin will probably change for both. Some users will want KeynesCoins and dump their MiltonBit holdings on exchange platforms or over-the-counter trades and vice versa. If a sizable chunk of bitcoiners choose team Keynes, then the price of MiltonBits might fall drastically. If the price of the tokens on open exchanges crumbles, so too could the mining power that safeguards the network against attack.

Rational miners will only spend electricity and capital up to the marginal revenue obtained from mining. If the price of the coin with respect to the cost of electricity and hardware declines, miners will probably take their mining machines offline, or if possible, dedicate their efforts to other more lucrative proof-of-work driven cryptocurrencies. If the total mining power on the network is low enough, a bad actor could corner the mining market more easily and attempt to disrupt the consensus system: block transactions at will, reverse transactions throughout the period in which they have control of the majority mining power, etc.

To round up this forking discussion, we can make the following general observation about trust in public consensus-driven networks. These systems do not create absolute trust or absolutely true computation; they merely generate a single source of truth that is trustworthy (A) only amongst participants who choose to remain compatible with their fellow participants and (B) only so long as a majority of those participants are behaving honestly. These systems do not fully obviate the need for "trust," but instead minimize the amount of trust necessary to a presumption that others will continue to run the software you also want to run, and no party will gain sufficient computational resources or stake sufficient wealth to dominate and then manipulate a leader lottery or other decision rules described by that software.

Consortium systems may be similar in that generally they are only trustworthy so long as a majority of identified consortium members are behaving honestly, and will only function if all members continue to run compatible software. However, we must also consider the entity that

identifies and then grants credentials to the consortium members. If this identifying member is corrupted, it could potentially shift the balance of power by granting more participatory rights to one or another consortium member than was assumed to be fair and agreed upon by the other members. The sanctity of a lottery or any other decision rule is only upheld by trust in an identifying agent and the safekeeping of identity credentials by participants (rather than by provable sacrifice of resources by participants). As the developers of Monax, a permissioned blockchain platform, explain:

The security model for permissioned blockchain networks is very similar [to public consensus networks], namely it is the non-predictive distribution of power over block creation among nodes unlikely to collude. Only, in a permissioned blockchain network the barrier to entry, and/or barrier to control, are provided either out of band by a previous or emergent agreement; added to the genesis block of the blockchain network and/or updated over time as different evolutions of the network become necessary. A possible attack vector at this point for overtaking a permissioned blockchain is thieving (or brute forcing) of 2/3rds of the private keys for the validator set.”⁶⁷

Additionally, the nature of an identified consortium may make it easier for some subset of the consensus members to find each other and collude to defraud the rest of the network (at least as compared with a network composed of pseudonymous participants with little or no information about their counterparties).

Finally, social consensus mechanisms are also trust-minimized but in a different manner than the other mechanisms. In a social consensus, you must trust some parties on the network, but need not trust all parties. To the extent that a global consensus is composed of some subset of data that the majority of all trusted participants have validated, we may worry that all participants are blindly placing trust in the same parties without careful consideration of how they should choose. If so, these trusted parties may be able to take advantage of this non-discriminating trust from the network at large and collude to defraud the network just as a majority group could do the same in the other mechanisms we’ve discussed.⁶⁸

iii. Trust for What Purpose?

To round up our discussion of trust, we also need to consider the question: *trust for what purpose?* Decentralized computing systems are potentially (and in some cases already are) useful for a variety of applications: peer-to-peer electronic cash,⁶⁹ identity,⁷⁰

⁶⁷ Monax, *What is a Permissioned Blockchain Network?*

https://monax.io/explainers/permissioned_blockchains/ last accessed Dec. 2016.

⁶⁸ Within the Ripple protocol this issue is, in theory, tempered because trusted validators will have reputations to uphold, and should any validator prove untrustworthy users will simply select alternative validators to place on their unique node list. Ripple Wiki: Consensus <https://wiki.ripple.com/Consensus> last accessed Dec 2016.

⁶⁹ See *infra* at 45.

⁷⁰ See *infra* at 51.

machine-to-machine payments in the Internet of Things,⁷¹ recording property rights,⁷² settlement of stock trades,⁷³ the settlement of accounts between large financial institutions,⁷⁴ and more.

In some applications where all participants are part of a tight-knit community with a limited goal (like settling accounts between banks for example), placing trust in an identified consortium and the party doing that identification may be entirely reasonable. Indeed, it may even be reasonable for the software that generates the consensus to be closed source as long as the identified participants (if not the larger public) feel satisfied that sufficient and independent audits of that code have been carried out to ensure that it does in fact do what its developers and vendors claim.

For other applications, however, trust in a central party may be sub-optimal. It could afford certain parties more power over our lives than we would ideally want. Public consensus models are by no means trustless, but they do decentralize power amongst a larger and open set of parties meaning that we are less likely to find ourselves (our transactions, our data, whatever we compute on the network) at the mercy of a single powerful institution that could either maliciously defraud us or negligently fail to maintain a secure network. There are three particular use cases of blockchains for which the trust-minimization inherent in a public consensus mechanism may prove critical: electronic cash, identity systems, and the internet of things. We discuss these in the final section. First, however, we need to discuss privacy.

C. Privacy Across Consensus Mechanisms

As we'll discuss in the final section, decentralized computing platforms may come to be the systems we use to safeguard our money, our identity, and our homes. Our daily activities, our credentials, and our transactions represent a wealth of personal data. The choice of consensus model can have repercussions with respect to our privacy. Who will be able to see your transactions if you use Bitcoin? Who will be able to see your comings and goings if you use a smart lock powered by Ethereum? Before we jump into the technical specifics, however, it's important to carefully describe what we mean by privacy, and what sort of privacy protection we would reasonably want or expect from decentralized computing systems.

i. Privacy and Context

Privacy is never absolute. Even a hermit who never speaks to anyone cannot avoid being seen

⁷¹ See *infra* at 58.

⁷² See Laura Shin, "Republic Of Georgia To Pilot Land Titling On Blockchain With Economist Hernando De Soto, BitFury" *Forbes* (Apr. 2016) <http://www.forbes.com/sites/laurashin/2016/04/21/republic-of-georgia-to-pilot-land-titling-on-blockchain-with-economist-hernando-de-soto-bitfury/#e5b6b4265500>.

⁷³ See John Detrixhe, "Scotland to Start Own Stock Exchange Using Blockchain Technology" *BloombergTechnology* (Oct. 2016) <https://www.bloomberg.com/news/articles/2016-10-27/scotland-to-start-own-stock-exchange-using-blockchain-technology>.

⁷⁴ See Gendal Brown *supra* note 7.

and scrutinized as she goes about her fishing, foraging or any of the other activities necessary to her survival. So rather than thinking about privacy as the mere ability to avoid public exposure or to keep secrets, let's think of it as the ability to control information about ourselves and our activities. This more nuanced concept is best described by Helen Nissenbaum's term *contextual integrity*.⁷⁵ Contextual integrity refers to the ability of an individual to control what information is released and what information is kept private depending on the context of a given social interaction.

Compare, for example, the information we'd want released to our dentist in advance of an appointment with the information we'd want released to our spouse in advance of a night out. These interactions have different contexts: medical and commercial vs. romantic and personal. Therefore, we cannot equate privacy with mere data security. Security simply means withholding some secret. Privacy means controlling to whom and in which situations we choose to reveal those secrets.

Whenever I interact with a decentralized system, I generate information that could become public. If the system is to protect my privacy, then ideally it would only share evidence of my interactions with the minimum set of participants necessary to accomplish my goals and expectations in interacting with the system. It should only share information that is relevant and appropriate within the context of the system as the user understands it.

An example makes this clearer: Let's imagine a system for transferring money. Alice gives money to Bob. Who needs to know what about this transaction? Of course, Alice and Bob need to know the amounts involved and who gets what. Bob also needs to know that the money Alice gave him is real and not a forgery, and he also needs to know that Alice truly gave up that money rather than retaining the ability to spend it. Finally, *everyone* who uses this particular sort of money needs to know that in this transaction no new money appeared unexpectedly, because if Alice somehow managed to both send the money as well as keep it for herself, then the supply of all money has grown and *everyone's* money will be worth a little less because of inflation.

Cash solves these problems by allowing the transaction to occur face-to-face between Alice and Bob. Bob can see that Alice has handed him a ten-dollar note. Bob knows he can walk away with the money and Alice won't be able to get it back. If they perform this ritual behind closed doors, no one else learns about the transaction. Cash notes are designed to make counterfeiting difficult, allowing *everyone* to know with some degree of certainty that no new money was created when Alice and Bob transacted.

Cash doesn't work online because a digital image of a ten-dollar note can be endlessly copied at effectively zero cost. Various solutions for moving money electronically have been developed but, of course, they vary in their ability to respect the privacy of the parties as

⁷⁵ Nissenbaum, Helen. "Privacy as contextual integrity." Wash. L. Rev. 79 (2004): 119. Available at: http://www.kentlaw.edu/faculty/rwarner/classes/internetlaw/2011/materials/nissenbaum_norms.pdf.

compared with cash.

Alice and Bob can use a bank or several banks in order to account for an electronic movement of money between them. Now Alice and Bob know what they need to know, but the bank also knows about the transaction. If the bank is hacked, the records of the transaction may become public knowledge. Despite having relatively little information to go on, *everyone* must be satisfied that the banks are keeping good records and that they are faithfully serving their role as lenders to maintain the relative scarcity and therefore price of the currency.

Bitcoin is a public consensus-driven peer-to-peer network that creates electronic cash for remote transactions without intermediaries like banks. Bitcoin provides Alice and Bob with the transactional information they need because they can (A) generate and agree on pseudonyms for each other, (B) view a global shared ledger that lists bitcoin balances for all pseudonyms, and (C) only spend balances on that ledger if they have a cryptographic key that matches the pseudonym. Bob knows that Alice has given up the funds because they've moved on the ledger to a pseudonym that only he controls. *Everyone* knows that no new money was created because they can see the transaction moved balances between two pseudonyms but did not create any new bitcoins. *Everyone* could also know the specifics of Alice's or Bob's transactions if the pseudonym(s) used by Alice or Bob can be linked to their name publicly.

Thus we see how three different system architectures (cash, electronic banking, and Bitcoin) all afford the relevant parties to the transaction varying levels of access to and control over the information created by, and necessary for, transacting.

ii. Privacy versus Transparency in Consensus

As we defined it, consensus is an agreement over (1) some set of data, (2) modifications to or computations with that data, and (3) the rules that govern that data storage and computation. An essential feature of these systems is that much of the activities of the participants will be fully transparent and verifiable to all participants in the consensus: the history of the data over which we are forming consensus is auditable and my modifications and computations with that shared data will be transparent so that my actions can be verified. It would be impossible for a network to ensure that the agreed upon rules for data storage and computation are being honored without some level of transparency.

To use Bitcoin as an example, if the full history of bitcoin transactions between users is not transparent, then I have no way of knowing whether a specific user purporting to send me five bitcoins has ever, herself, received or mined those five bitcoins. Similarly, if the transaction from this user to me is not incorporated in the ledger, no future recipient of the funds I've just been sent can be assured that I'm good for the money.

Bitcoin is able to have this level of transparency but still offer some privacy to its users because all of the entities transacting or mining bitcoin on the network are represented by pseudonyms. Specifically, to use Bitcoin I will have my Bitcoin software generate one or more public-private keypairs. The private key is the secret I need to have in order to sign for valid

transactions, and the public key is the address or account to which people can send me bitcoins. The public key is a pseudonym. My name may be Peter, but when I transact on the network other machines and users will recognize and address me only by a random string of text:

17kdugRB1fdvqFC1BHkBwjZWm2wbt982AH

The problem with this approach is that if anyone learns that I'm the real person behind 17kdug... then they can look up my full transaction history with that address. One solution has been to use several addresses and never reuse an old address. So everytime I ask to be paid, my Bitcoin software will create a new address for me to share with the payor,⁷⁶ and everytime I send bitcoin from an address, the remainder or "change" from the transaction is sent to a brand new address. Even with these procedures in place, however, my several addresses could still be linked and identified with forensic tools. For example, if I have two bitcoins each in three different addresses, and I want to pay someone five bitcoins, I will need to use all three of my addresses in order to fund the transaction. With all three of these addresses listed as inputs to the transaction, a nosey person looking at the blockchain can easily assume with some certainty that those three addresses were all one person, me. If any of those addresses have been previously marked as belonging to me, then we're back at the initial problem: my full transaction history is potentially public information.

The same privacy problem is generalizable to any sort of decentralized computing platform powered by the consensus mechanisms we have so far discussed. The need for transparency and verifiability may conflict with our desire for privacy as we use these systems. As we'll see there are two general approaches to resolving or ameliorating this conflict: *perimeter security* and a variety of new techniques, which we can call *data minimization*.

iii. Perimeter Security versus Data Minimization and Selective Disclosure

Faced with an essential trade-off wherein verifiability requires transparency but privacy requires that user-data remain opaque, there are essentially two design options:

1. **Perimeter Security:** Leave all data relevant to the consensus transparent but restrict the set of parties who verify that data to a local and private group of verifiers with whom you are comfortable sharing otherwise private data.
2. **Data Minimization:** Develop tools to only reveal data essential to group consensus if it is absolutely necessary to verification and allow the group of verifiers to be open and global.

Perimeter security follows an older approach in network security generally: *if there are things to be kept secret, we build a secure perimeter, restrict the flow of sensitive information to within*

⁷⁶ This is not as inconvenient as it may seem. The wallet software that I use should keep track of all of these addresses and keep the associated private keys secured in a single file (if I'm securing my own bitcoin) or else a company can keep track of this data on my behalf. Either way, when I transact I don't need to worry about a number of addresses and keys, I just spend bitcoins from my wallet.

*that perimeter, only allow authorized parties into that perimeter, and carefully monitor for and prevent breaches.*⁷⁷

Data minimization takes an alternative approach: *we will not rely on a secure perimeter, all information in the system can be presumed to be global and available, but the only information ever put into the system is the minimum amount of information necessary to accomplish the goal.*⁷⁸

Again, an example will make this distinction clearer. Alice wants to send money to Bob, but wants privacy. A money transmission system with perimeter security would look rather like existing mobile payment applications like PayPal or Venmo. Alice and Bob share the full private details of their transactions with a single verifier, e.g. PayPal. PayPal allows Bob to know that Alice has a sufficient balance to send the money, ensures non-repudiation, and by balancing its books gives the public the assurance that no new money was created out of thin air (it was only transferred). As long as PayPal maintains a secure perimeter, the details of these transactions remain private. The downside of this solution is two-fold: (1) we now cannot rely on the larger public to verify the details of the transaction, we must trust the party or group that is within the perimeter (e.g., Paypal), and (2) if the perimeter is ever breached, then all of this data could become public.

A money transmission system employing data minimization instead of a secure perimeter model would look rather like an improved version of Bitcoin. Recall that within Bitcoin, all details of the transactions are public but they are pseudonymous. We have previously discussed how this pseudonymity can be weak and result in the public revelation of an individual user's full transaction history. A system like Bitcoin with more robust data minimization would limit the public data to information that is relevant to consensus and allow the users to choose what additional information they would like to reveal about their specific transaction. Here's what that could look like:

Information Alice needs to know: An address where she can pay Bob, confirmation that Bob got paid (in case he tries to claim he didn't).

Information Alice does not need to know: the balance of Bob's address(es) before or after the transfer.

Information Bob needs to know: That he's been paid, and that the payment is genuine (the

⁷⁷ See Lenny Zeltser, Karen Kent, *et al.* "Perimeter Security Fundamentals" *Inside Network Perimeter Security* (Apr. 2005) chapter available at <http://www.informit.com/articles/article.aspx?p=376256>.

⁷⁸ See generally Peter Schaar, "Privacy by Design" 3 *Identity in the Information Society* 2 (Aug. 2010) available at <http://link.springer.com/article/10.1007/s12394-010-0055-x/fulltext.html> discussing the concept of data minimization within the context of Privacy by Design, i.e. "The idea of incorporating technological data protection" into the overall design of an application or computer system, "instead of having to come up with laborious and time-consuming 'patches' later on. ... Privacy by Design goes beyond maintaining security. Privacy by Design includes the idea that systems should be designed and constructed in a way to avoid or minimize the amount of personal data processed. Key elements of data minimization are the separation of personal identifiers and content data, the use of pseudonyms and the anonymization or deletion of personal data as early as possible."

sender has enough money to fund the transaction).

Information Bob does not need to know: the name of the sender, the balance of the sender's address(es) before of after the transfer.

Information the whole network (the public) needs to know: That money was transferred but was not created.

Information the whole network does not need to know: Any identities (including pseudonyms) involved in the transfer, or the specific amounts that were involved in the transfer (because these can potentially also be used to identify the transaction).

From this baseline of privacy, the parties should also be able to *voluntarily* choose to be less private. This choice is referred to as *selective disclosure*.⁷⁹

Alice should be able to choose what otherwise private information she'd like to selectively disclose:

- She can choose to let Bob know the payment was from her and should be able to prove to Bob (using the verification power of the entire network that she is the one who paid him).
- She can choose to let particular third parties (or the public at large) know the details of the transaction (her name, Bob's name, and/or the amount that was paid).

Bob should be able to choose what otherwise private information he'd like to selectively disclose:

- He can choose to let third parties know the details of the transaction (his name, the amount he was paid, and—if Alice shared this information with him—Alice's name).

Similarly, Bob should be able to reject payments if he'd like, this way Bob can refuse to accept a payment from someone who did not identify herself to him. While these disclosures are voluntary as far as the software is concerned, they may be required by law.⁸⁰

This same selective disclosure paradigm could be highly useful in other consensus-driven systems aside from value-transfer, for example identity: a customer should be able to present

⁷⁹ See Zooko Wilcox and Paige Peterson, "The Encrypted Memo Field" *Zcash Blog* (Dec 2016) <https://z.cash/blog/encrypted-memo-field.html>.

⁸⁰ See, e.g., Zooko Wilcox and Peter Van Valkenburgh, "What is Zcash" *Coin Center* (Dec 2016) <https://coincenter.org/entry/what-is-zcash> ("whenever the law demands transparency and whenever proper legal process is followed to obtain that transparency, a user or regulated firm can easily oblige by sharing the view key that un-blinds private transactions with the proper authorities. This is, in many ways, superior to the current state of affairs with Bitcoin where both law enforcement and the general public can see a wealth of private information about your Bitcoin addresses. It's also better than the current state of affairs with pre-blockchain banking transactions because the data being shared can be verified by an open network of computers, rather than law enforcement needing to take the regulated party or the individual being questioned at their word.").

a bartender with an attestation token that proves that an attestor (e.g., the Department of Motor Vehicles) has verified that she's old enough to legally drink, but that token and the decentralized computing system that powers it should not inadvertently disclose her name, address, or anything else about her to the bartender unless she wants to reveal that information.⁸¹

This architecture has significant advantages over perimeter security. Unlike perimeter security, the choice of remaining private does not come at the cost of trusting a party or a group within a secure perimeter. The validity of the transfer, the fact that no new money was created, and that the transfer cannot be reversed, can all be public information guaranteed by an open set of validators rather than be facts we need to trust a private set of validators to be honest about. Also, with data minimization and selective disclosure there is no central perimeter to be hacked. It's possible that the credentials I use to choose my level of selective disclosure could one day be hacked, and the hacker could reveal all of my transaction records, but there is no central perimeter that, if hacked, would reveal *all private transactions from all users* of the system. The negligence of one user, employee, or vendor partner (failure to set a strong password, willingness to open strange attachments in phishing emails, etc.) does not automatically jeopardize the entire system.⁸²

iv. Perimeters or Minimization Techniques in Consensus Mechanism Design

It has been suggested that public consensus mechanisms (i.e., proof-of-work, proof-of-stake, and social consensus) are not suitable for enterprise or financial sector applications because they are not sufficiently private.⁸³ It is true that Bitcoin presents us with an example of this weakness: pseudonyms are too easily identified and transaction histories of users are too vulnerable to public scrutiny. However, faced with this dilemma, there are a variety of solutions. The commonly cited solution is to build only private, consortium consensus-driven

⁸¹ David Birch has worked diligently to articulate this notion of data minimization and transactional identity. As Birch frames it: "What is needed to enable transactions is not identity per se but the associated entitlements." Not, "I am John Doe" but instead "I am old enough to order this beer." Birch calls this form of identification

"pseudonyms with credentials." David Birch, *Identity is the New Money* (2014).

⁸² Take for example the 2015 Target breach. At Target, consumer credit card credentials were stored on an internal server, but hackers did not initially infiltrate this server. Instead, they targeted a vulnerable server controlled by a heating and cooling company that Target used as a facilities services vendor. By granting some network access to this vendor, Target unknowingly and unintentionally extended the network of trust to which its customers belonged. Once the heating and cooling company was compromised, so was Target and so were all of their customers. With enough new and variable links in a chain, one is likely to be weak enough to unravel the whole. See Brian Krebs, "Target Hackers Broke in Via HVAC Company," *KrebsOnSecurity* (Feb. 2015)

<http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/>.

⁸³ See, e.g., ESMA, Discussion Paper: The Distributed Ledger Technology Applied to Securities Markets (Feb. 6, 2016) https://www.esma.europa.eu/sites/default/files/library/2016-773_dp_dlt.pdf ("We understand that the DLT [distributed ledger technology] that is likely to be applied to securities markets would be 'permission-based' in contrast to the 'permissionless' system that was originally designed for virtual currencies, e.g., Bitcoins, for a number of reasons, including efficiency, security and privacy purposes.")

networks for these use-cases. The only privacy gain inherent to this approach is the creation of perimeter security. For example, the banking technology consortium R3 has described its Corda decentralized ledger product as follows:

“The foundational object in our concept is a state object, which is a digital document which records the existence, content and current state of an agreement between two or more parties. It is intended to be shared only with those who have a legitimate reason to see it.”⁸⁴

Privacy is thus ensured by sharing the “state object” only with one’s trusted counterparties, with those “who have a legitimate reason to see it.” The agreement is made private by placing it behind a secure perimeter, not necessarily by limiting the contents of the agreement to data relevant to consensus over that agreement. If any of the “legitimate” parties are compromised, the contents of the agreement could become public. In this sense the consortium model on its own does little to change the state of information security beyond what we see from existing centralized financial intermediaries. Indeed, it may be on balance a more vulnerable system because the secure perimeter now includes employees at other firms. Additionally, if the entire contents of the agreement are private to the relevant parties, independent validation of the data cannot occur in a fully trust-minimized manner (*i.e.*, from an open and global network of impartial transaction validators); one only gets validation from the set of parties permitted by the consortium to enter the secure perimeter.

To R3’s credit, it is investigating various other approaches to better enhance privacy as described in their near- to mid-term roadmap:

Privacy enhancements using technology such as address randomization,
zero-knowledge proofs.⁸⁵

These are approaches that apply equally well in consortium and public consensus-driven systems. Significantly, these technologies have been primarily pioneered in the Bitcoin and related cryptocurrency communities.

Address randomization is effectively the attempt to create more robust pseudonyms that fail to yield to forensic identification techniques. Most research into the development of these techniques is occurring in the Bitcoin space where, without robust address randomization, privacy is fairly poor as previously described. Notable pioneering advances in this approach are the CoinJoin⁸⁶ and Coin Shuffle⁸⁷ protocols, which create decentralized communications

⁸⁴ Corda Introductory Whitepaper (Aug. 24, 2016)
<http://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/57bda2fdebdbd1acc9c0309b2/1472045822585/corda-introductory-whitepaper-final.pdf>.

⁸⁵ *Id.*

⁸⁶ Blockchain.info, SharedCoin and other CoinJoin implementations: Uses and Limitations (June 10, 2014)
<https://blog.blockchain.com/2014/06/10/sharedcoin-and-other-coinjoin-implementations-uses-and-limitations/>.

⁸⁷ Tim Ruffing, Pedro Moreno-Sanchez, and Aniket Kate, CoinShuffle: Practical Decentralized

channels to facilitate the shuffling of bitcoins between several addresses in a manner that makes it difficult to link a set of addresses to one particular user. Additionally, changes to the Bitcoin core protocol have been researched and proposed that would obscure the value of each transaction as it appears in the blockchain, a project referred to as Confidential Transactions.⁸⁸ Simultaneously, some security researchers have proposed that key concepts from the Confidential Transactions and CoinJoin protocols, could be combined and used to obscure both the value and the participants to a transaction. This new research has been referred to, whimsically, as Mumblewimble (from the Harry Potter books) and it is now being developed into a standalone cryptocurrency called Grin.⁸⁹

Separately, Zero-knowledge proofs are a cryptographic tool for proving some important fact (e.g., this transaction is valid, these bitcoins have never been spent by this sender before), without revealing any other information aside from the proof.⁹⁰ Integrating zero-knowledge proofs into a public consensus blockchain could potentially allow a decentralized open set of transaction validators to prove that all recent transactions have been appropriately funded, signed, and not double-spent, without revealing any additional information about who sent how much to whom. The Zcash Electronic Coin Company has been pioneering these technologies in the form of Zcash, a public consensus (proof-of-work) driven digital currency network. Not only is Zcash testing the viability of a truly data-minimized approach to privacy and consensus, the protocol also allows users to selectively disclose information about their transactions to whomever they choose.

Zcash transactions automatically hide the sender, recipient and value of all transactions on the blockchain. Only those with the correct view key can see the contents. Users have complete control and can opt-in to provide others with their view key at their discretion.⁹¹

Still another cryptographic tool that can be utilized to provide privacy alongside reliable verification of data on a public blockchain is a ring signature. Briefly, these signature schemes can be employed to prove that one of several members of a group authoritatively signed a message without revealing which member of the group actually did the signing. Ring signatures are already employed by the cryptocurrency Monero to protect user privacy.⁹²

These systems are in many ways ideal: Trust in the scarcity of the underlying tokens and the non-reputability of transactions is generated by an open set of impartial validators (rather

Coin Mixing for Bitcoin <https://crypsys.mmci.uni-saarland.de/projects/CoinShuffle/coinshuffle.pdf>

⁸⁸ “The Elements Project Confidential Transactions,”

<https://www.elementproject.org/elements/confidential-transactions/>

⁸⁹ “Grin, the Tech,” <https://grin-tech.org/>

⁹⁰ See Wilcox *supra* note 79.

⁹¹ Giulio Prisco, Zcash Creator on the Upcoming Zcash Launch, Privacy and the Unfinished Internet Revolution (Aug. 30, 2016)

<https://bitcoinmagazine.com/articles/zcash-creator-on-the-upcoming-zcash-launch-privacy-and-the-unfinished-internet-revolution-1472568389>.

⁹² “Ring Signature,” *Moneropedia*, <https://getmonero.org/resources/moneropedia/ringsignatures.html>.

than a consortium of identified but potentially corrupt or infiltrated parties). Privacy is guaranteed by neglecting to share any information about transactions with these validators except for the minimized amount of information necessary to prove scarcity and non-repudiation. Additionally, selective disclosure ensures that counterparties and third parties can be given visibility into the details of any particular transaction whenever the initiator wishes to be transparent or is compelled to be transparent by regulation or investigation.

IV. Use Cases in which Public Consensus is Critical

There are many use cases or applications that can be created and deployed equally well on public or private blockchain networks. There are, however, certain use cases that can only achieve their full potential if they use a public and permissionless blockchain network. These use cases for which public consensus is critical, not coincidentally, also happen to be at the fundamental level of information systems: identity, security, and payments.

The most obvious use case in which public consensus is critical is in building *general purpose* decentralized computing networks—the decentralized computing platforms discussed at the start of this testimony. Just as the Internet has become a public platform for the proliferation of innumerable useful applications dealing primarily with communication of information, so too could networks like Bitcoin, Ethereum, Zcash, Monero, or Grin become platforms for innumerable applications dealing primarily with recordkeeping, exchange, and governance. The principle advantage of using public consensus mechanisms to form the basis of these platforms is the dynamism and diversity inherent in an open ecosystem of application developers, where developers need not seek permission to tinker with, create, and test a new idea.

But speaking abstractly of a variety of applications that will presumably emerge in a non-permissioned environment is not particularly satisfying. So for the remainder of this testimony we will discuss three specific, promising use cases that would particularly benefit from being built on top of public platforms.

The three use cases we will highlight can all be thought of as *applications*, a word we have thus far thrown about haphazardly without definition. By applications we mean *human jobs or problems that benefit from computing*. At the start of each subsection we will specify the specific human job or problem under discussion, and then go on to explain why that application would benefit from being built on top of a public consensus mechanism rather than a private and permissioned system.

A public consensus mechanism decentralizes trust, spreading out power on the network across a larger array of participants. In general, decentralization helps ensure **user sovereignty**, **interoperability**, **longevity**, **fidelity**, **availability**, **privacy**, and **political neutrality**. These attributes will be explained in the context of each application, and a discussion of public and private consensus mechanisms for that application will follow.

Speaking generally, however, and abstracting away some technical nuance, public consensus mechanisms are critical in use cases where any of these attributes are desirable because only by including the user's device or an unbounded set of disinterested proxies for that user's interests in the consensus mechanism (by designing that mechanism such that *anyone* can participate and not just an empowered few) can the user free themselves from reliance on a single centralized counterparty to guarantee their privacy, the longevity of the network, the fidelity of the data in the blockchain, etc.

Again, public consensus mechanisms and the scarce tokens (like bitcoin or ether) that incentivize participation in the consensus, are not merely an artifact of the political biases of the initial creators of these technologies, they are also essential to the well-functioning of any system that desires user empowerment. So in the cases discussed below—electronic cash, identity, and the Internet of Things—we will explain why individual user empowerment is essential to the use case, and therefore, why public consensus mechanisms like proof-of-work or proof-of-stake are essential to building the infrastructure that powers those consumer or business applications.

A. Electronic Cash

Bitcoin was the original blockchain and public consensus mechanism, and the white paper that first described the invention clearly describes the application it promised: “A purely peer-to-peer version of electronic cash [that] would allow online payments to be sent directly from one party to another without going through a financial institution.”⁹³ Note that the design is more specific than often reported. Bitcoin was not designed to be a settlement tool for financial institutions, a lending or borrowing tool, a register for financial instruments, or a repository for any other sort of data. Bitcoin was designed to do one thing: enable cash-like (as in similar to paying with paper notes) transactions on the Internet.

i. What is Cash? Why is it Difficult Online?

Cash is a settlement tool, a very simple one that we tend to take for granted. Say I owe you \$20 because you are a restaurateur who's just provided me with an excellent lunch. I have a debt that I can now settle very easily if I have cash: I hand you a \$20 bill; done.

The peculiar utility of cash is derived from it being a fungible bearer instrument. A *bearer instrument* simply means that whoever holds the instrument is entitled to the rights described in the instrument.⁹⁴ The rights described by a \$20 note were, historically, redemption by a bank or government of an equal amount in “real money” like gold coinage. The transition to fiat money altered that right subtly to redemption of any equally sized debt, public or private. In either case the possessor of the right is whoever holds the \$20 note. *Fungible* means that any particular \$20 note carries the same rights as any other \$20 note (indeed two \$10 notes

⁹³ See Nakamoto *supra* note 26.

⁹⁴ See William E Britton, “Transfers and Negotiations Under the Negotiable Instruments Law and Article 3 of the Uniform Commercial Code” 32 Tex. L. Rev. 153 (1953-1954).

together carries the same rights as well).

Fungible bearer instruments reduce transaction costs within any economic exchange.⁹⁵ In the midst of any given transaction, say paying the tab at a restaurant, neither party needs to pause and inquire as to the provenance of the note, whether it rightfully belonged to the buyer according to some authoritative registry of notes, or whether this particular note is blacklisted by virtue of being used previously in a crime or pledged as collateral in some ill-fated loan. Instead, the buyer presents the note, it looks like any other note, and would—as any other note—buy as much lunch. The transaction happens fluidly and without delay because the parties do not need to engage in fact finding or deep contemplation about the medium of exchange presented. Transaction costs are minimized. This particular reduction in transaction costs has long been understood as essential to a well-functioning economy. Take, for example, a report of the policy arguments made in a formative Scottish case on the subject of bank notes and fungibility in 1749:

Policy issues, as might be expected, were highly prominent in Lord Strichen's Report. Trade, it was argued for the Banks, rested on the free circulation of money, and free circulation rested in turn on the reliability of notes and coins. If Crawford [the plaintiff, a previous holder of a bank note, and from whom the note in question was stolen] was able to vindicate the banknote, no merchant could risk taking money in payment 'without being informed of the whole History of it from the Time that it first issued out of the Bank or the Mint till it came to his Hand, which is so apparently absurd, that it seems hardly to merit a Consideration'. And as banknotes would thus be rendered 'absolutely useless', this would 'in a great Measure deprive the Nation of the Benefit of the Banks, which could hardly subsist without the Circulation of their Notes'. It was in vain for [opposing counsel] to object that, just as people continue to buy goods despite the (slight) risk that they might be stolen and subject to vindication, so they would continue to accept money if the risks were the same. If money could be vindicated, counsel for the Bank of Scotland concluded, 'no Man could be sure, that one Shilling in his pocket was his own, and ... Banks might shut their doors.'⁹⁶

Crawford lost his case and the fungibility of cash was guaranteed by the courts in Scotland. Similar decisions followed in other jurisdictions, and the fungible paper currency we know and rely on to this day was assured.

Compared with cash, pre-Bitcoin online transactions had relatively high transaction costs. This is because all electronic instruments are, effectively, registered instruments rather than bearer instruments. A *registered instrument* means that the rights associated with the

⁹⁵ See generally, David Fox, *Property Rights in Money*, §§ 2.11–2.20 (2008).

⁹⁶ See Kenneth Reid "Banknotes and Their Vindication in Eighteenth-Century Scotland" *University of Edinburgh, School of Law, Working Papers* (Nov. 2013) http://www.research.ed.ac.uk/portal/files/13523302/Reid_Banknotes.pdf. *quoting* Lord Strichen, Reporter, *Minutes, the Governor and Directors of the Bank of Scotland against the Governors and Directors of the Royal Bank and others* (21 February 1749).

instrument adhere only to the person whose name appears in some authoritative register, the current bearer of a particular certificate or note related to that instrument is irrelevant.

The reason why electronic instruments must be registered is straightforward. Digital files, like Microsoft Word documents or MP3 music files, can be costlessly duplicated. While the reproduction of a music CD will necessarily entail the costs inherent in the production of another physical thing, digital music files can be replicated with almost no effort or expense. If the bearer of a particular file is entitled to rights described in that file, and any person can almost costlessly copy the file again and again, then it is trivial to effectively manufacture more rights. A \$10 file on my computer, if copied over and over can become a billion dollars. To address this, banks or other intermediaries will keep a centralized record (*i.e.*, a registry or ledger) of who has which rights to which electronic funds. If I claim to pay an online retailer, the retailer's computer effectively calls up my bank to make sure I have the money I say I do.

These registered instruments require mutual trust in the ledger keeper. If I'd like to pay you electronically, we'd both need to have an account at the same bank or else use an additional intermediary, like a correspondent bank or a credit card company, who can be a trusted go-between for our particular banks.

All of these intermediaries generate transaction costs. The magnitude of these costs will depend on the efficiency of the intermediaries, and the number of intermediaries necessary to build a trustworthy bridge between myself and the person I'm paying. Each may take a fee; each will take their time to process the transaction.

There are also hidden costs in these systems: chargebacks, and transactions forgone. Credit cards, for example, may appear to offer near instant transactions, but in reality the credit card company only *authorizes* future payment between the banks of the parties. If when that future payment goes to be settled (and even after the settlement), it turns out that the card has been reported stolen, the merchant receiving the payment may suffer a chargeback (*i.e.*, they will not receive the sum they were promised and they will bear the loss of the real goods they gave in exchange).⁹⁷ Additionally, when transaction costs are high, small-value transactions become cost-inefficient and people will simply avoid making them. This is the case with microtransactions to pay for or meter low-value digital goods (*e.g.*, a minute of Wi-Fi at the airport, the ability to read just one article on a pay-walled website).⁹⁸ Another substantial hidden cost is the unavailability of electronic payment to those who cannot obtain a banking relationship. Several billion people across the world do not have banking relationships, often through no fault of their own.⁹⁹ Banks will frequently deem a prospective customer's personal

⁹⁷ When goods are purchased using stolen credit cards, the merchant is generally left taking the loss. The Bureau of Justice Statistics estimates that these losses cost Americans over \$24.7 billion in 2012 alone. That's 10 Billion more in losses than all other property crimes combine." See Bureau of Justice Statistics, Data Collection: National Crime Victimization Survey (NCVS) (2012) *available at* <http://www.bjs.gov/index.cfm?ty=dcdetail&iid=245>.

⁹⁸ See Chris Smith, "What are Micropayments and How does Bitcoin Enable them?" *Coin Center* (June 2015) <http://coincenter.org/entry/what-are-micropayments-and-how-does-bitcoin-enable-them>

⁹⁹ Asli Demirguc-Kunt, Leora Klapper. Dorothe Singer, Peter Van Oudheusden, "The Global Index

characteristics or the country where they reside as too indicative of risk for them to be profitable customers.¹⁰⁰ Women and other vulnerable groups are disproportionately affected by bank de-risking.¹⁰¹ For these people, online transactions are simply not an option and the full global costs of these transactions-forgone goes uncounted.

ii. Why Public Consensus is Critical for Cash

In a metaphysical sense, even paper bearer instruments exist on a “register” of sorts, but that register is global, decentralized, and easily made transparent. The register is the world of physical possession. Reading from the register looks like this: *whose hands or pockets hold which instruments?* And writing to it looks like this: *accept the note from the person who is handing it to you.* It is similar with bitcoin, but instead of hands and pockets and the physical world we have software and a global network. Bitcoin’s key innovation was to *simulate* a bearer instrument digitally by using networked software to fully automate and decentralize the registry of instruments, such that the “registry” component of the instrument effectively fades into the background. My bitcoins are still described on a register and that’s why I can’t duplicate them willy-nilly, but the register is merely an unowned, shared, and ubiquitous feature of networked computers (just like the Internet is an unowned, shared, and ubiquitous communications feature for most computers today—and just like the ability to exchange paper notes or stuff them into wallets or safes is a ubiquitous feature of the physical world). When I transact with bitcoins I don’t need to consider the blockchain or peer-to-peer networking

Database 2014 Measuring Financial Inclusion around the World” *World Bank Policy Research Working Paper* 7255 (April 2015) available at

<http://documents.worldbank.org/curated/en/187761468179367706/pdf/WPS7255.pdf#page=3>.

¹⁰⁰ See Tracey Durner and Liat Shetret, “Understanding Bank De-Risking and its Effects on Financial Inclusion” *Oxfam Research Report* (Nov. 2015) available at

https://www.oxfam.org/sites/www.oxfam.org/files/file_attachments/rr-bank-de-risking-181115-en_0.pdf. (“As financial institutions re-calculate risk appetites and decide to exit relationships, they directly and negatively affect these sectors and the populations they serve. For example, in August 2014, Westpac Banking Corp. followed other major Australian and UK banks and announced the closure of numerous money transfer operators’ accounts over concerns about AML/CFT and rising compliance costs. This followed the precedent set in the wake of Barclays’ May 2013 decision to close money transmitter accounts and the subsequent temporary injunction filed by Dahabshiil, one of the largest Somali remittance companies in the UK. The closure of these bank accounts not only threatens these businesses but also jeopardizes the vital flow of remittances to Somalia from diaspora populations, which constitute an estimated 25 to 45 percent of the country’s GDP and serve as a key source of income for more than 40 percent of its vulnerable population.”)

¹⁰¹ *Id.* at 6 (“For example, in developing countries, 46 percent of men have a bank account, compared to 36 percent of women. Immigrants are another heavily affected population: factoring out socioeconomic and demographic considerations, immigrants are six percent less likely to have a checking account and eight percent less likely to have a savings account in the US than their American-born counterparts. Without formal bank accounts, these underserved populations commonly rely on the remittance sector to send money to their families back home, and women have increasingly emerged as a key sending demographic. Although they remit about the same amount as men, women are shown to remit higher percentages of their income, more frequently, and for longer durations than their male counterparts. Reductions in the remittance sectors due to MSB account closures stand to further isolate these communities from the global financial system, exacerbating existing financial inclusion challenges.”).

technology, just as when I visit a website I don't need to contemplate TCP/IP or HTTP.

To truly fade into the background, that system must exhibit certain qualities that real-world cash possesses:

Some qualities exhibited by physical cash:

- **User sovereignty:** The choice to initiate a cash transaction is entirely up to the person holding the cash. No intermediaries need be relied upon to ensure that the transaction can proceed.
- **Availability:** Cash transactions are always available. If you have cash on you, you can hand it to someone else.
- **Interoperability:** Within a given nation, everyone accepts and recognizes the value of cash. In the international context, the availability of liquid foreign exchange markets and the availability of a global reserve currency generally guarantees some level of global interoperability.
- **Longevity:** Cash has no expiration date, notes that have been hanging around in a mattress for years work just as well as fresh bills. Purchasing power may fluctuate over time but should not go to zero.
- **Fidelity:** Cash is designed to be difficult to counterfeit and to make counterfeit notes more obvious to the would-be recipient.
- **Political neutrality:** While the value of cash ultimately relies in part on its supply (a factor at least roughly controlled by governments and large banks) the ability to transact with cash is not contingent on any government or corporation. A holder of cash can hand that cash to another person without first seeking the approval of the issuing bank or government.
- **Privacy:** Cash transactions do not create a record.

Electronic cash powered by a public consensus mechanism simulates these qualities:

- **User sovereignty:** The bearer of a private key that corresponds to a pseudonym in control of some bitcoins is the only party able to initiate transactions and no particular transaction validator need be relied upon to ensure that the transaction can proceed.
- **Availability:** No particular transaction validator can block a user perpetually from transacting, nor would the technical failure of any particular validator stop the user from transacting because the process of writing and reading from the digital ledger is decentralized across a public network of peers, any of whom could serve as a validator.
- **Interoperability:** I don't have to have a common relationship with a particular validator and the person I'm paying in order to pay; all software necessary to utilize and interact with the network is freely available without seeking licenses or paying fees. While many may not immediately recognize the value of a bitcoin or other unit of electronic cash, the availability of liquid exchange markets generally guarantees some level of interoperability.

- **Longevity:** By decentralizing the storage of the ledger redundantly across all participants, and employing digital signatures to link all transactions into a unified data structure, the network ensures that even very old transactions never go missing from the ledger. Balances a user has left untouched for years or even decades are still available for spending.
- **Fidelity:** Transactions are recorded on the ledger in bundles called blocks. Transactions must obey logical rules to be incorporated into blocks (e.g., spending the same bitcoins twice is not allowed). Transactions cannot be altered after the fact; any such attempted alteration would invalidate digital signatures within the block containing the transaction and in all subsequent blocks. These mismatched signatures highlight the fraud and (unless the full network of participants decide to change the network's rules against fraud) the attempt at alteration would be ignored. New transactions might be "erased" in favor of other transactions when one "block" replaces another within the most recent history of the ledger, but blocks further back in the ledger cannot be replaced without simultaneously replacing all blocks since that block, a process that would demand prohibitively costly computing resources.
- **Political neutrality:** By creating a public and global market for transaction validation and infrastructure upkeep, the network ensures that it would never be vulnerable to attempts by one government or institution to censor or stop particular transactions, or freeze particular balances. Additionally, the supply of the tokens is set by the software, and so would not be subject to the monetary policies of a state or the choices of a single corporation or institution.¹⁰²
- **Privacy:** Bitcoin transactions *do* leave a record, but it is a pseudonymous record that generally does not make a user's full transaction history public information. The development of privacy-protecting technologies like zero-knowledge proofs or shuffling protocols may make identification of pseudonyms more difficult while also granting individuals the ability to selectively disclose information related to their transactions.

Private consensus mechanisms would make it difficult to guarantee these features:

- **User sovereignty:** The user must rely on the consortium members as intermediaries to ensure that the transaction will proceed.
- **Availability:** The identified members of the consortium could be compromised and the system could cease validating transactions or could be made to block the transactions of certain users. If the members collude they could block the transactions of certain users.

¹⁰² Centralization of validators on an open network because of economic advantages from cooperation or geographic co-location is a real concern in these systems, however, thus far we've see little evidence of harms from this vulnerability. See Kyle Torpey, "Problems Associated With Bitcoin Mining Centralization May Be Overstated" *Bitcoin Magazine* (Sep. 2016) <https://bitcoinmagazine.com/articles/problems-associated-with-bitcoin-mining-centralization-may-be-overstated-1474917259>.

- **Interoperability:** Identified members could choose to only validate transactions from their collective customers, transactions between the users of one consortium's network and those of another may be more difficult or impossible.
- **Longevity:** The permanence of the balances on the ledger is guaranteed by the goodwill and the security practices of consortium members. If the ledger is not public, alterations or omissions could occur without scrutiny.
- **Fidelity:** Without a public ledger, users must trust the consortium members to vouch for the validity of any particular transaction history. Even if the ledger is regularly published by the consortium members and incorporates digital signatures, there is no process in place to reconcile discrepancies between the currently authoritative record endorsed by the consortium and some other version that, according to some users, proves that alterations have been made.
- **Political neutrality:** Consortium members retain the ability to censor transactions or blacklist specific funds, and censorship may be carried out for political purposes.
- **Privacy:** Transactions create a record that may or may not be pseudonymous. The privacy of this record is only guaranteed by the good faith and good technical practices of the consortium.

Only public consensus-driven networks can deliver the streamlining provided by true cash transactions. Instruments registered to a public blockchain can be treated as if they were bearer instruments because the process of updating the register is automated and decentralized: user sovereignty, availability, interoperability, longevity, fidelity, political neutrality, and privacy are effectively guaranteed by cryptography and economic incentives for honest participants.

If there is doubt about that automation, or if a set group of entities must be trusted to accomplish that purported "automation," the signed transactions cannot be treated as fungible bearer instruments. As in the case of credit card authorizations, we might fear repudiation if the automation is not guaranteed. As in the case of the unbanked, we might fear that some parties would be denied access to the system or have their transactions momentarily frozen because the trusted parties deem them too much of a risk. As in the correspondent banking context if the trusted parties refuse to make the register fully transparent or interoperable with other registers, we might fear that easy transactions can only be had between parties who have become customers of the same consortium.

Fundamentally, from a user perspective, a private blockchain technology doesn't "just work" from the get-go. I cannot send or receive money until I open an account and establish a legal relationship with a company. This may be a tolerable inconvenience, but it is not a system that works like cash, which can be accepted in the hand without any prior arrangements in place.

Only by fully automating the creation and maintenance of a ledger according to pre-established rules and economic incentives that play out in a public market for transaction validation can we be sure that electronic transactions are as good as cash.

B. Identity

The Internet lacks a native identity layer. This shortcoming is the reason why Internet users must rely on a tapestry of weak passwords, secret questions, and knowledge of mother's maiden names to verify their identity to various web service providers. The need for a better solution is widely recognized,¹⁰³ and public blockchains may provide the answer.

i. What is Identity? Why is it Difficult Online?

In the physical world, identity is *federated*.¹⁰⁴ In other words, we don't have just one monolithic identity; we have a host of attributes. Nor do we have just one institution that vouches or attests that we have these attributes, we have several. A person's identity includes an endless variety of attributes: physical appearance, parentage and family history, citizenship, educational and employment history, skills, personality, etc. We seek and often carry evidence that others have attested to our attributes: driver's licenses, passports, birth certificates, membership cards, diplomas, letters of recommendation, professional certifications, awards, resumes, etc. In the physical world our identity is *user sovereign*: the bulk of these credentials are things over which we have immediate physical control; we keep them in our homes or our wallets; we might even wear them on our faces. We are in control of these attestations and can choose to show or decline to show them to others at will.

Online we should expect no different. As early as 1996, the need for robust digital identity systems was glaringly apparent. As the Clinton Administration noted in its Framework for Global Electronic Commerce:

Of particular importance is the development of trusted certification services that support the digital signatures that will permit users to know whom they are communicating with on the Internet. Both signatures and confidentiality rely on the use of cryptographic keys. To promote the growth of a trusted electronic commerce environment, the Administration is encouraging the development of a voluntary, market-driven key management infrastructure that will support authentication, integrity, and confidentiality.¹⁰⁵

But creating a robust, federated, and user-sovereign identity system that works online has proven difficult. As President Obama noted in a letter introducing the National Strategy for Trusted Identities in Cyberspace ("NSTIC") program:

The rapid and vastly positive changes that have followed the rise of online transactions — like making purchases or downloading bank statements — have also led to new

¹⁰³ See, e.g., Barak Obama, *Cover letter to the National Strategy for Trusted Identities in Cyberspace* (April 2011) available at https://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

¹⁰⁴ See Eve Maler and Drummond Reed, "The Venn of Identity: Options and Issues in Federated Identity Management" *IEEE Security & Privacy* (2008) available at <https://css.csail.mit.edu/6.858/2012/readings/identity.pdf>.

¹⁰⁵ See Clinton *supra* note 8.

challenges. Few have been as costly or nerve wracking for businesses and families as online fraud and identity theft. These crimes cost companies and individuals billions of dollars each year; and they often leave in their wake a mess of ruined credit and damaged finances that can take years to repair. But there are other costs for our economy that are more difficult to measure. The potential for fraud and the weakness of privacy protections often leave individuals, businesses, and government reluctant to conduct major transactions online. For example, providing patients with access to their medical records from their home computers requires that hospitals be able to confidently identify that patient online.

The simple fact is, we cannot know what companies have not been launched, what products or services have not been developed, or what innovations are held back by the inadequacy of tools, like insecure passwords, long overwhelmed by the fantastic and unpredictable growth of the Internet.¹⁰⁶

One of the key challenges has been developing an interoperable system for online identity. As the NSTIC framework specifies:

The third guiding principle of the Identity Ecosystem is to ensure policy and technology interoperability among identity solutions, which will enable individuals to choose between and manage multiple different interoperable credentials. Interoperability will also support identity portability and will enable service providers within the Identity Ecosystem to accept a variety of credential and identification media types.¹⁰⁷

Interoperability is a technical challenge that demands a public, purpose-neutral platform through which users and institutions can present credentials and offer attestations depending on their particular needs. Researchers at Microsoft have stressed that:

[D]ifferent identity systems must exist in a metasytem. It implies we need a simple encapsulating protocol (a way of agreeing on and transporting things) ... The universal identity metasytem must not be another monolith. It must be polycentric (federation implies this) and also polymorphic (existing in different forms). This will allow the identity ecology to emerge, evolve, and self-organize. Systems like RSS and HTML are powerful because they carry any content. We need to see that identity itself will have several—perhaps many—contexts, and yet can be expressed in a metasytem.¹⁰⁸

Another key challenge lies in creating a system that is privacy-protecting. As the NSTIC framework specifies:

Just as there is a need for methods to reliably authenticate individuals, there are many

¹⁰⁶ See Obama *supra* note 103.

¹⁰⁷ *Id.*

¹⁰⁸ Kim Cameron, *The Laws of Identity* (May 2005)

<https://msdn.microsoft.com/en-us/library/ms996456.aspx>.

Internet transactions for which identification and authentication is not needed, or the information needed is limited. *It is vital to maintain the capacity for anonymity and pseudonymity in Internet transactions in order to enhance individuals' privacy and otherwise support civil liberties.* Nonetheless, individuals and businesses need to be able to check each other's identity for certain types of sensitive transactions, such as online banking or accessing electronic health records.¹⁰⁹

This mirrors our discussion of privacy as contextual integrity. Depending on the circumstance, the user of the system should be empowered to control what identity information they reveal and what they keep secret. The goal of the system is, as was discussed in the context of zero-knowledge proofs, selective disclosure. Such a system cannot rely on perimeter security, obscuring private information by hiding it behind a firewall or using proprietary security software, in order to protect privacy. As researchers at Microsoft have stressed:

Since the identity system has to work on all platforms, it must be safe on all platforms. *The properties that lead to its safety can't be based on obscurity or the fact that the underlying platform or software is unknown or has a small adoption.*¹¹⁰

Another key challenge has been creating a truly user-sovereign system. As the NSTIC framework stresses:

Individuals shall be free to use an Identity Ecosystem credential of their choice, provided the credential meets the minimum risk requirements of the relying party[.] Individuals' participation in the Identity Ecosystem will be a day-to-day—or even a transaction-to-transaction—choice.¹¹¹

Given these particular demands from online identity—interoperability, user sovereignty, and privacy—it should be increasingly apparent why public consensus mechanisms would be preferable in the development of online identity systems.

ii. Why Public Consensus is Critical for Identity

One way to look at Bitcoin is as a system that allows an otherwise anonymous individual to prove that they have a certain amount of funds without revealing any other personal details about themselves.¹¹² The same technology could be leveraged to prove all sorts of attributes

¹⁰⁹ See Obama *supra* note 103.

¹¹⁰ See Cameron *supra* note 108.

¹¹¹ See Obama *supra* note 103.

¹¹² I can sign a statement that indicates I have control over some subset of my bitcoins, let's say 5. You can see that statement (or use software to read a verify it) and note that it is signed with the key that matches a public address on the blockchain, which has had 5 bitcoins sent to it in past transactions. I have proven that I control these 5. However, I may have other address that have more bitcoins. In this manner, a blockchain can be used to prove some limited facts about me without revealing more information about myself than I'd prefer. It is true that Bitcoin's blockchain currently leaks additional information about me, because clustering analysis may allow a stranger to determine the balances of all of my addresses (rather than only the address I've signed a message using) if my addresses have been

about an individual, effectively creating a user-sovereign, federated identity system.

Already some companies are experimenting with such a system. Today, for example, I can use a service called Onename, created by a company called Blockstack, to leverage the Bitcoin blockchain in helping me establish an online identity.¹¹³ It works like this: I log into my Facebook account, my Twitter account, and my LinkedIn account and post a special message proving I control those accounts. A copy of that message is then signed with a digital signature that matches my established Bitcoin address.¹¹⁴ Proof of those signatures can be encapsulated in the Bitcoin blockchain and the Onename website will make it easy for me to sign, write, and read those messages to and from the blockchain. Now, if I want to prove to someone who I am online, I can show them my signed messages on the blockchain and sign a personal message to them using the same key.

Effectively, the system allows the user to self-attest to an identity. The user shows that they have control over three different social networking profiles by creating signed attestations on each profile. A single Facebook account may be easy to fraudulently generate, but three different social media accounts, particularly if they have active use indicative of the person they purport to represent, would be harder to forge. With attestations from each account now available on the blockchain, we can be reasonably assured that any message signed with the private key matching that blockchain address is truly a message from the person who has those social media accounts.

We could imagine similar attestations from any number of federated attestors also residing as signed messages encapsulated and stored on the Bitcoin blockchain or any other public consensus blockchain. Now if want to prove I have a certain credit score, or a certain diploma, I can ask the credit rating agency or the university to sign an attestation and “transfer” it (as one would transfer bitcoins) to a public blockchain address I control. Now I can present that attestation, signing it again with my private key, to anyone curious about my creditworthiness or educational history. Because blockchains provide a sort of decentralized time-stamping, the attestation could be made to expire automatically, and subsequent on-chain messages signed by the attestor could revoke previous attestations if, say, my credit score changes or if my diploma is revoked.

These attestations could also be required of users who want to log into a given website, say an online banking account. Rather than mandating that a user create a password and use that password to log in, a bank could sign a login credential and assign it to that user’s blockchain address. Now, to log in, she signs a login message with the private key that matches her blockchain address. The bank’s website looks for that signed message, validates the signature,

used together in past transactions. This privacy weakness is, however, surmountable and, as discussed in the section on privacy (*see infra* at 35), several efforts are underway to make public blockchain networks more private, and capable of true granular information sharing and verification.

¹¹³ See Ali *supra* note 5. See also <https://onename.com/>.

¹¹⁴ See, e.g., my personal Onename profile: <https://onename.com/valkenburgh> and an associated message I placed on my twitter profile: <https://twitter.com/valkenburgh/status/595664205270880258>.

and allows her to login. Reverse engineering a Bitcoin private key is effectively impossible, and that's a major step up from most user-set passwords that can be cracked in hours or even minutes by an enterprising hacker.

If the user loses her phone or laptop, her private keys could, of course, be compromised, and if she failed to keep backups she will be unable to sign messages proving her identity attestations. To solve this problem, public blockchain networks can leverage what are called multi-signature transactions. In essence, before accepting any attestation credentials at a given blockchain address, I empower three friends, co-workers, or institutions, with the ability to re-assign my credentials to another address should I ever lose my keys. Now if I lose my cell phone, I can call up my friends, ask them to revoke my credentials, and then meet with them to provision those credentials to a new address I've generated with the keys stored on my new device.

As with our discussion of electronic cash, it's now helpful to describe the key attributes offered by **public consensus mechanisms** and explain how they relate to an online identity system:

- **User sovereignty:** The bearer of a private key that corresponds to a pseudonym in control of certain identity attestations is the only party able to offer an attestation as proof of her identity, and no third party aside from the attester who issued that attestation need be relied upon to ensure that the identification can proceed.
- **Availability:** No particular node on the network can block a user perpetually from offering attestations for identification purposes, nor would the technical failure of any particular node stop the user from offering attestations because the process of writing and reading from the digital ledger is decentralized across a network of peers.
- **Interoperability:** The user does not have to have a common relationship with any particular member of the network and the person to whom they are identifying themselves for an attestation to be shared; all software necessary to utilize and interact with the network is freely available without seeking licenses or paying fees. The user can seek attestation credentials from any individuals or institutions that choose to use the system and there is no fee or permission or establishment of any provider-customer relationship required for an attester to join the system and start making attestations about users.
- **Longevity:** By decentralizing the storage of the attestations redundantly across all participants, and employing digital signatures to link all attestation transactions into a unified data structure, the network ensures that even very old attestations never go missing from the ledger. Attestations a user has left untouched for years or even decades are still available for proving her identity (provided they have not been set by the attester to expire).
- **Fidelity:** Attestations are recorded on the ledger within transactions that are bundled into blocks. Transactions and their associated attestation data cannot be altered after the fact; any such attempted alteration would invalidate digital signatures within the block and in all subsequent blocks. These mismatched signatures highlight the fraud and the attempt at alteration will be ignored. New attestations might be "erased" when

one “block” replaces another within the most recent history of the ledger, but blocks further back in the ledger cannot be replaced without simultaneously replacing all blocks since that block, a process that would demand prohibitively costly resources in a proof-of-work or proof-of-stake consensus mechanism.

- **Political neutrality:** Attestation credentials are added to the system using the same transaction writing and transaction validation techniques employed by current bitcoin transactions. By creating a public and global market for transaction validation and infrastructure upkeep, the network ensures that it would never be vulnerable to attempts by one nation to invalidate attestations or revoke identities without the consent of the attestor.¹¹⁵
- **Privacy:** Writing attestations *does* leave a public record of a person’s identity, but it is a pseudonymous record that generally does not make a user’s full identity (all of her attestations) public information. The development of privacy-protecting technologies like zero-knowledge proofs or shuffling protocols may make identification of pseudonyms more difficult while also granting individuals the ability to selectively disclose information related to their identity (e.g, prove to a bartender that they are over 21, but avoid showing them irrelevant additional information such as name or address).

Private consensus mechanisms would make it difficult to guarantee these features:

- **User sovereignty:** The user must rely on the consortium members as intermediaries to ensure that attestations about them are made and incorporated into the system or shared with other users.
- **Availability:** The members of the consortium could be compromised and the system could cease offering access to attestations, or could be made to embargo the attestations possessed by certain users. If the members collude they could block the user from identifying herself to other users.
- **Interoperability:** Consortium members could choose to only permit attestations by certain institutions, and could forbid attestations to be made about their own customers. Identification verification between the users of one consortium’s network and those of another may be more difficult or impossible.
- **Longevity:** The permanence of the attestations on the network is guaranteed by the goodwill and the security practices of consortium members. If the attestation data and associated digital signatures are not public, alterations or omissions could occur without scrutiny.
- **Fidelity:** Without a public record of attestations, users must trust the consortium

¹¹⁵ Centralization of validators on a public network because of economic advantages from cooperation or geographic co-location is a real concern in these systems, however, thus far we’ve see little evidence of harms from this vulnerability. See Kyle Torpey, “Problems Associated With Bitcoin Mining Centralization May Be Overstated” *Bitcoin Magazine* (Sep. 2016) <https://bitcoinmagazine.com/articles/problems-associated-with-bitcoin-mining-centralization-may-be-overstated-1474917259>.

members as to the validity of any particular attestation. Even if the record of attestations is regularly published by the consortium members and incorporates digital signatures, there is no process in place to reconcile discrepancies between the currently authoritative record endorsed by the consortium and some other version that, according to some users, proves that alterations have been made.

- **Political neutrality:** Consortium members retain the ability to censor identity attestations, block user from asserting their identities, or blacklist specific users/identities, and censorship may be carried out for political purposes.
- **Privacy:** Writing attestations creates a record of users' identities. The privacy of this record is only guaranteed by the good faith and good technical practices of the consortium members.

In general, identity is a many-faceted concept. A person's identity is a bundle of qualities that she exhibits, and attestations that others make about her. If a centralized authority can see as well as revoke any and all of your credentials, it could present privacy and human rights issues. No such singular authority exists in the physical world where even a person denied a driver's license can still obtain a diploma, where a person denied a bank account can still get a passport, where the common infrastructure of identity is paper, plastic cards, or independent electronic records. We should expect nothing less from the digital world, and public consensus mechanisms are essential to that development.

C. The Internet of Things

The promise of the Internet of Things is that every device you own or use—every “thing” in your home and beyond—will be “smart” and “networked.”¹¹⁶ From light switches to door locks, thermostats to toothbrushes, street lights to cars, everything will be collecting data about its use, will have a networked interface for remote usage, and will be able to communicate as needed with users or any other devices with which it may need to coordinate. Self-driving cars will whiz through intersections because their trajectories will be intelligently coordinated with other vehicles, refrigerators will know when you are running out of eggs or when the milk's gone bad and will order more, and every appliance in your home will be able to be switched off from hundreds of miles away if you're on vacation and worried you left something on.

Whether this utopian vision is likely or even desirable goes beyond the scope of this paper. Many homes already have smart thermostats, lights, door locks, televisions, and voice assistants like Amazon's Alexa, and even with these non-speculative, early-generation IoT devices, the need for public networks to underpin their operation is becoming apparent. Additionally, non-consumer, industrial IoT usage is on the rise. For example, smart devices can enable the automated monitoring of well-head flows across an oil field, equipment safety across a construction site, or soil moisture across a farm.¹¹⁷ These uses also face the same security, availability, and longevity concerns as consumer devices but the consequences of

¹¹⁶ See IBM *supra* note 58.

¹¹⁷ See Saint-Andre *supra* note 56.

failure can be even more dire.¹¹⁸

i. Why Public Consensus is Critical for the Internet of Things

IoT devices in general will need to identify themselves online for control and communications purposes. This means that all of the concerns we had about human identification in the previous section are again present with respect to device identification. IoT underscores the importance of decentralized identity because rather than merely being concerned with some 10 billion people who may each have multiple digital credentials (*e.g., can drive, is over 18, or has credit score 729*) we must now also consider that each person may have 10 or even 100 smart devices in their home, business, or under their control, and each device may have multiple identities and credentials (*e.g. this lock can be opened by these five family members and this friend and these emergency personnel in case of an emergency, or this car must be capable of communicating with and then programmatically sharing the road with every other car that may be traveling today*). The sheer number of device identities and credentials inherent in projections of widespread IoT deployment necessitates that no one or handful of centralized authorities be in full control of that identification system. Reliance on one or a handful of identity validators would invite fragility into a massive and critical technological system; it would entrust reams of private data to a small group of actors who could engage in abusive or anti-competitive business practices or else become the target of devastating hacks.

Similarly, devices may need to shop and make payments. This is already the case for voice assistants like Amazon's Alexa, which can be used to shop for and buy consumer goods by voice interaction alone. This brings us back to several of the issues we encountered in the section on electronic cash. Payments, including device payments, should be under the control of the person whose value is at stake, the user. A device manufacturer need not retain the ability to block payments or accumulate private payments-related data merely because they sold you a piece of IoT hardware. A ride-sharing application developer should not necessarily retain the ability to limit your selection of possible drivers or prices merely by limiting the markets for drivers that your smartphone is capable of accessing. Consumer choice, privacy, and payment security can be bolstered if our connected devices can shop for us via decentralized markets powered by decentralized payment systems.

In previous sections we've looked at seven attributes of public consensus mechanisms and investigated how a particular use case may require these attributes. Rather than rehash all seven attributes here again, this section will focus on four that have particular importance in the IoT context: longevity, user sovereignty, privacy, and interoperability.

Longevity. A recurring annoyance for IoT pioneers (brave souls who have, say, already replaced all of their lightbulbs with smart bulbs) is unexpected or rapid "sunsetting" of a product by its manufacturer. This refers to a decision by the manufacturer to end technical or infrastructural support for the product. Within the realm of non-smart products, an end to

¹¹⁸ See, *e.g.*, Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon" *Wired* (Nov. 2014) <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>.

manufacturer support can already be troublesome because customer service and repair may now become more difficult, but in the realm of smart products an end to support can be significantly worse.

A smart product will often only function properly when it is capable of connecting to and communicating with a server on the Internet that may, among other things, (A) help it identify itself and connect to other consumer products or Internet services,¹¹⁹ (B) provide a web- or app-based user interface for the user to control the product's features,¹²⁰ and/or (C) store and process data essential to the device's operation.¹²¹ That server will generally be operated and maintained by the device manufacturer and, should the manufacturer decide to take that server offline, the device may cease proper operation. This has been the case even with seemingly simple smart home products like light bulbs.

Take for example issues surrounding bulbs manufactured by Connected by TCP.¹²² These bulbs were marketed as being compatible with other smart-home systems, in particular the Amazon Echo voice assistant (so that you could say, e.g., "Alexa, turn on my kitchen lights")¹²³ and a mobile app called Wink that offers a dashboard for user control over a variety of smart devices (so that you would not need to navigate to various different apps on your phone to control devices made by different manufacturers).¹²⁴ The bulbs were also marketed as being capable of remote control over the Internet (so that you could turn them on and off even when out of the range of your home Wi-Fi network). Compatibility and remote control for the Connected by TCP bulbs was provided via a web server that was owned, maintained, and under the full control of Connected by TCP. The server would relay signals for switching the bulbs on and off from a user's Amazon Echo or Wink app to the user's Connected by TCP light bulb hub, and then, in turn, to the bulbs themselves.

In June of 2016, after years of selling these bulbs, Connected by TCP abruptly decided to take their server offline.¹²⁵ With the critical relay path to the bulbs now missing, all remote functionality and device interoperability disappeared. As a writer for Consumerist wrote:

The bulbs still work as actual lightbulbs, if you want to use your lamp's on-off switch the old-fashioned way, and you can control them while inside the house on your home

¹¹⁹ See Tobias Heer, *et al.*, "Security Challenges in the IP-based Internet of Things" *Wireless Pers Commun* (2011) available at <http://link.springer.com/article/10.1007/s11277-011-0385-5>.

¹²⁰ *Id.*

¹²¹ *Id.*

¹²² See Kate Cox, "TCP Disconnects "Smart" Lightbulb Servers, Leaves Buyers In The Dark" *Consumerist* (Aug. 2016) <https://consumerist.com/2016/08/19/tcp-disconnects-smart-lightbulb-servers-leaves-buyers-in-the-dark/>.

¹²³ See Michael Garcia, "Using Alexa Skills Kit and AWS IoT to Voice Control Connected Devices" *Amazon Developer* (May 2016) <https://developer.amazon.com/blogs/post/Tx3828JHC7O9GZ9/Using-Alexa-Skills-Kit-and-AWS-IoT-to-Voice-Control-Connected-Devices>.

¹²⁴ "Wink Hub" *Wink.com* <http://www.wink.com/products/wink-hub/> last accessed Dec. 2016.

¹²⁵ See Cox *supra* note 122.

WiFi network. But any remote functionality—a big part of the steep price tag that makes TCP bulbs more expensive than a plain old LED bulb—is long gone.

The fact that the bulbs are still on store shelves, with packaging promising features that no longer exist, is irksome. But it's also not an uncommon tale in these early years of the Internet of Things. Businesses try, and then discontinue, new products all the time.¹²⁶

The Federal Trade Commission has taken a careful look at this burgeoning problem, launching an investigation into Google's choice to end support for products manufactured by Nest, a smart-home firm it acquired.¹²⁷ The FTC ultimately closed that investigation but warned manufacturers of their concern over two key policy issues:

First, there are serious issues at play when consumers purchase products that unexpectedly stop functioning due to a unilateral decision by the company that sold it. Consumers generally expect that the things they buy will work and keep working, and that includes any technical or other support necessary for essential functioning.

Second, when a company stops providing technical support, including security updates, for an IoT device, consumers may be left with an out-of-date product that is vulnerable to critical security or privacy bugs. This could create vulnerabilities for other systems connected to these IoT devices, and put consumers' sensitive data at risk. And if hackers can hack a smart car, pacemaker, or insulin pump, the risks are even more serious.¹²⁸

Public consensus mechanisms can provide significantly enhanced longevity by replacing a privately owned and maintained server with a decentralized computing network. Device identity and data storage can be offloaded to a decentralized ledger and decentralized file system and the device can even be pre-loaded by the manufacturer with a modest amount of funds to pay the global network of parties contributing resources to that decentralized network for the device identity registration, data storage, and connectivity that it needs for a reasonable lifetime. Now, even if the manufacturer goes out of business, if it decides to change its product offerings, or is acquired by a company unwilling to continue device support, the device itself will continue to have the same network infrastructure necessary to maintain proper functioning.

A private consensus mechanism may not provide this guarantee of longevity. The consortium members, just like the company with a centralized server, may choose to deprecate support for older products, or they may shut down the network entirely. Only a public network where participants are free to come and go and are incentivized to participate by device payments

¹²⁶ *Id.*

¹²⁷ Jessica Rich, "What happens when the sun sets on a smart product?" *FTC Business Blog* (Jul 2016) <https://www.ftc.gov/news-events/blogs/business-blog/2016/07/what-happens-when-sun-sets-smart-product>

¹²⁸ *Id.*

will assuredly continue to function for as long as devices continue to pay. Additionally, if the device's on board wallet is pre-loaded with electronic cash powered by a public blockchain network, then reloading the device with new funds is a simple process that anyone in possession of the device (perhaps even after multiple resales) could accomplish.¹²⁹

User sovereignty and privacy. Nobody wants a baby monitor, security camera, or even a remote-activated light bulb that several dozen complete strangers may be able to access and control. In the world of “dumb” devices this was easy for a device designer to avoid: unless you have physical access to the switches on the device, you have no control over its operation. So a baby monitor that is closed-circuit or that only broadcasts analog signals will generally be in the sole and sovereign control of people in the house. Assume there are locks on the doors and we have good user-sovereignty and privacy.

Smart, internet-connected devices, however, when they rely on web servers for their functionality, will often fail to have these qualities. Recall Nick Szabo's characterization of the web's client-server architecture:

When we currently use a smartphone or a laptop on a cell network or the Internet, the other end of these interactions typically run on other solo computers, such as web servers. Practically all of these machines have architectures that were designed to be controlled by a single person or a hierarchy of people who know and trust each other. From the point of view of a remote web or app user, these architectures are based on full trust in an unknown “root” administrator, who can control everything that happens on the server: they can read, alter, delete, or block any data on that computer at will.¹³⁰

This applies to any device in the home that connects to the Internet as well as it does to a smartphone or laptop. Let's imagine a baby monitor that can be switched on and off remotely, and that broadcasts audio and video to the user's smartphone. Generally, these devices are manufactured to use a client-server architecture.¹³¹ The logic of the application (rules for how and when the device should turn on, rules for who has access to the device, rules for how data from the device should be routed) exists on a server controlled and maintained by the device manufacturer and physically remote from the device (probably in a large data center somewhere).¹³²

The user connects the baby monitor to the Internet using the home's wired or Wi-Fi connections and the device, in turn, connects to the manufacturer's web server; the baby monitor is now one client of the server. The user then sets up her smartphone with an app provided by the manufacturer for controlling the baby monitor and viewing the feed. The user's device is *another* client of the server. When the user decides to switch on the monitor from her cell phone, a message is sent to the server, checked for authenticity, and then relayed

¹²⁹ See *infra* at 45.

¹³⁰ See Szabo *supra* note 2.

¹³¹ See Heer *supra* note 119.

¹³² *Id.*

to the device itself. The baby monitor turns on. Unlike a light switch that completes a circuit entirely within the home, this “circuit” exists across potentially hundreds of miles of Wi-Fi, cellular signal, satellite, fiber-optic cable, and server warehouse. Similarly, when the baby monitor relays a video feed of baby, that data travels back across the Internet, to the server, and then back to the user’s device (this may be the case even when the user is in her own home and near the monitor).

This system architecture presents a major issue from a user-sovereignty standpoint. Unless the application server is very carefully designed, someone with physical access to that server may be able to control the baby monitor as easily as the user can from her cell phone. Indeed, if the application server is poorly designed (e.g. firewalls are not well employed, user passwords are not strong and properly stored, encryption is not used to mask data coming and going from the server, and/or streaming protocols are employed without password-protection) then anyone in the world with an Internet connection may be able to control the baby monitor.

This is not as rare of problem as it may sound. Indeed, there is a search engine, Shodan,¹³³ that can be used to comb the Internet for connected devices that promiscuously broadcast unprotected video feeds, as reported by Ars Technica:

Shodan, a search engine for the Internet of Things (IoT), ... includes images of marijuana plantations, back rooms of banks, children, kitchens, living rooms, garages, front gardens, back gardens, ski slopes, swimming pools, colleges and schools, laboratories, and cash register cameras in retail stores, according to Dan Tentler, a security researcher who has spent several years investigating webcam security. "It's all over the place," he told Ars Technica UK. "Practically everything you can think of."¹³⁴

Off-loading as much device registration and application logic as possible to decentralized systems should provide enhanced user-sovereignty. This may be relatively straightforward when it comes to authentication. As discussed in the section on identity, the user can provision herself (e.g. her smartphone) and the smart device with identity credentials and access rules that would reside on the blockchain. The device can always query the blockchain for a current list of authorized users (e.g., pseudonyms that must sign with matching private keys to gain access) and users can rely on multi-sig setups to revoke credentials if their smartphone is lost or stolen.

Data from the device, say video feeds from a security camera, can be encrypted and stored locally or in a decentralized file system¹³⁵ where members of the network provide surplus storage in return for payments from devices. So long as the keys to the encrypted data remain

¹³³ Shodan, <https://www.shodan.io/> last accessed Dec. 2016.

¹³⁴ J.M. Porup, “*Internet of Things’ security is hilariously broken and getting worse*” ArsTechnica (Jan. 2016) <http://arstechnica.com/security/2016/01/how-to-search-the-internet-of-things-for-photos-of-sleeping-babies/>.

¹³⁵ See, e.g., IPFS, <https://ipfs.io/> last accessed Dec. 2016.

with the user, none of these otherwise anonymous storage providers will be able to access or view the encrypted files.

Computing tasks that the device may need to perform in order to function, say analyzing video data to find human faces or identify intruders, can be designed to run locally on the device only, rather than on a server. Alternatively, those computing tasks could also be offloaded to a decentralized computing network¹³⁶ where participants offering computing services are rewarded by payments from the device for data processing. In this case, of course, no private data should be shared with the decentralized network unless it is encrypted. This may appear to limit the value of a decentralized computing network: how can the network process the data if it cannot view it unencrypted? The science of distributing computing work amongst several participants without fully revealing encrypted data data is a vibrant and growing subfield within cryptography, generally referred to as *secure multiparty computation*.¹³⁷

One technique in this field is the development of robust *homomorphic encryption*,¹³⁸ which means that a computation performed on an encrypted file will yield the same result as a computation performed on a plain text (not encrypted) file. So in our video analysis example, the decentralized network can still process the video data and give a result: *in this 12 hours of video there was one human intruder who entered the house*, but the various maintainers of the several computers that may have been involved in that decentralized data processing cannot ever see the unencrypted video file and therefore cannot ever see any details about the device-user's home (aside from knowing that there was one human intruder within a given time, as per our example).

Zero-knowledge proofs provide another cryptographic tool used to achieve this level of privacy.

¹³⁹ As described previously, a ledger of transactions can be effectively encrypted or hidden but a zero-knowledge proof can still process the data in that ledger and reveal whether any transactions attempted to double spend funds. In this sense a public ledger can still be privacy protecting while still guaranteeing that all transactions were valid and not counterfeit. This can work in the IoT context as well. Rather than "all transactions were valid," the limited proof is "all smart lock door openings were from authenticated users," and only this data becomes public not the specific times that the door was opened or the identities of the authorized lock openers.

Another tool to build these system architectures is the division of computational work into several small pieces and the assignment of that work across several unaffiliated participants none of whom can see the entire file being processed and, therefore, see the private data undergoing computation. The Enigma Project out of MIT is an effort to build just such a secure

¹³⁶ See, e.g., Ethereum, Buterin *supra* note 6.

¹³⁷ See Yehuda Lindell and Benny Pinkas, "Secure Multiparty Computation for Privacy-Preserving Data Mining" *Journal of Privacy and Confidentiality* (2009) available at <http://repository.cmu.edu/cgi/viewcontent.cgi?article=1004&context=jpc>

¹³⁸ See *id.* at 79.

¹³⁹ See *id.* at 76.

multi-party computation system that relies on a blockchain to divide work into pieces, keep track of the pieces, find participants, and assign work among them.¹⁴⁰ This avoids reliance on a single trusted intermediary to achieve the division, a potential vulnerability if that intermediary can reassemble the pieces and see the private data being processed.

In general, the computation, data storage, and network access rules currently found within a server-client architecture for smart home devices could be decentralized by using public consensus mechanism driven networks. In theory, a private consortium driven network could achieve similar results. However, this reintroduces trust in the identified members of the consortium, weakening the goal of pure user-sovereignty.

Interoperability. Smart devices need to interact with other smart devices. The door sensor needs to communicate with the smart bulbs in order to make the hall lights come on if you come home after dark. Self-driving cars need to communicate with other self-driving cars if they are going to have smart collision avoidance and traffic pattern automation. An Amazon Alexa or similar voice controlled assistant needs to communicate with digital music retailers in order to let you shop for new music by voice.

Herein lies, perhaps, the most common sense argument for using public consensus mechanism networks to power devices in the Internet of Things. If the infrastructure powering a smart device is owned and controlled by one particular manufacturer, integrating that device with other devices may be difficult. Worse, that integration may be made deliberately difficult to gently cajole the customer into buying all of their devices from one manufacturer. This is the issue of so-called *walled gardens* in computing systems: everything is beautifully manicured but you can't leave.¹⁴¹ If customers cannot choose competing products without suffering the substantial switching costs inherent in replacing *all* of their IoT devices, free and open competition suffers, and prices rise.¹⁴²

This is particularly the case with devices that deal with online shopping. Take Amazon Echo for example. This voice assistant allows the user to order products merely by asking for them. Simply say, "*Alexa, buy me some cat litter!*" and the device will look at your past shopping habits, propose a brand, amount, and price, and allow you to agree or ask for another option. There is a fascinating and undeniably convenient feeling associated with truly hands free shopping.

But, of course, having an Alexa in your home will mean you are locked in with one retailer, Amazon, for any and all hands-free shopping that you do. When Alexa queries your shopping history and the varieties of cat litter on offer, she only shops Amazon's suppliers and partner merchants. Similarly, if you ask Alexa to play music, she will only be able to play songs you

¹⁴⁰ Guy Zyskind, Oz Nathan, Alex "Sandy" Pentland, *Enigma: Decentralized Computation Platform with Guaranteed Privacy*, (Dec. 2015) http://www.enigma.co/enigma_full.pdf

¹⁴¹ See Richard Firth, "Beware the walled gardens" *itWeb Open Source* (Mar. 2013) http://www.itweb.co.za/index.php?option=com_content&view=article&id=62788.

¹⁴² See Carl Shapiro & Hal r. Varian, *Information Rules: A Strategic Guide To the Network Economy* 109-10 (1998) (discussing strategies to deter customer mobility by imposing switching costs).

bought or uploaded to your Amazon account; she can't play from the collection you've amassed on, for example, iTunes. Ideally, a device would be able to access any of the digital property the user has previously purchased, and it should comparison shop across all willing sellers for things the user has yet to buy, selecting the best price for the item she wants. This open competition can only be achieved if the markets for buying and selling are truly decentralized.

Several firms are building the tools to accomplish just such decentralized commerce; one that warrants highlighting in this testimony is OpenBazaar.¹⁴³ OpenBazaar is, in essence, a decentralized eBay where buyers and sellers can find each other and engage in a safe exchange. Buyers and sellers are protected from fraud on OpenBazaar by leveraging multi-sig bitcoin transactions to place funds in a sort of trust-minimized escrow while goods are in transit or being evaluated for quality. In the event of a dispute a neutral third party arbitrator is invoked who can redirect the funds to either the seller or the buyer based on their decision regarding who was in the wrong in the disputed transaction. Additionally, OpenBazaar uses BlockStack's decentralized identity tools to create and authenticate the identities of buyers and sellers, and may soon use a decentralized files system, IPFS,¹⁴⁴ to host images and descriptions of items listed for sale. The result is an online shopping experience just like eBay, but it can exist on decentralized network where there is no company like eBay that has any control over the sales that occur on their platform.

There is not a good case for using regulation to force device manufactures to participate in public decentralized markets; walled gardens can have their appeal and regulations can have unintended consequences. However, it's important for policymakers to understand the potential value decentralized networks provide in fostering open digital exchange and commerce that could be foundational to better, future IoT systems.

Altogether, the case for having public consensus mechanisms power IoT blockchain networks is clear and linked to our prior discussion of identity and electronic cash. First, public blockchain networks allow for a truly decentralized data-structure for device identity (I am a bulb in this home) and user access authorization (user with address 0xE1A... is the only person who can turn me on and off). The redundant and decentralized nature of data on these networks can ensure that these systems have true longevity, and a manufacturer's decision to end support for a product will not destroy the user's ability to securely access the product's features. Second, public blockchain networks can ensure that devices are interoperable and compatible because critical infrastructure for device communication, data storage, and computation can be commoditized and shared over a peer-to-peer network rather than be owned (as a server warehouse is owned) by a device manufacturer that may be reticent to opening its costly platform to competitors. Third, device payments for supporting and maintaining that networked infrastructure or allowing the device's user to easily engage in online commerce can be made efficient by utilizing the electronic cash systems that only

¹⁴³ OpenBazaar, <https://openbazaar.org/> last accessed Dec. 2016.

¹⁴⁴ IPFS, <https://ipfs.io/> last accessed Dec. 2016.

public consensus mechanisms can facilitate.

V. Conclusion

All new approaches to decentralized computing—whether private or public—should be celebrated and allowed to develop relatively unfettered by regulatory or government policy choices. Much as the Clinton Administration took a light-touch approach to the development of the Internet in the 1990s, so should policymakers approach these new systems, however designed.¹⁴⁵

In order to make good policy choices and ensure that the U.S. remains competitive in a global technological market we need a more detailed and productive discussion of these new tools. We need a basic understanding of how consensus works, what it might help us build, and why public and pseudonymous networks, despite their easily apprehended risks, offer significant and otherwise unattainable benefits. This testimony has offered a non-technical explanation of key variables within consensus mechanism design, catalogued why public mechanisms may, for certain use cases, be more worthy of user trust and more capable of ensuring user privacy and security.

The benefits of this technology are real. Electronic cash promises efficient microtransactions and enhanced financial inclusion; robust digital identity may solve many of our online security woes and streamline commerce and interaction online; and blockchain-driven Internet of Things systems may spur greater security, competition, and an end to walled gardens of non-interoperability for connected devices. However, our three highlighted use cases are likely only the tip of the iceberg. Just as few would have predicted the emergence of Facebook or Uber given only an understanding of the Internet circa 1995, it is impossible to know what creative and diverse minds will build when offered a free and public platform for experimentation.

¹⁴⁵ See Clinton *supra* note 8.

IRS signals retreat in court battle that could reshape block reward taxation

Newly minted crypto should be taxed at sale, rather than creation

by Peter Van Valkenburgh February 3, 2022

Last year, Joshua Jarrett sued the IRS for a refund. In 2019 he earned block rewards on proof-of-stake networks, paid taxes as if those rewards were income (as per the limited guidance we have so far from the IRS), but also asked for a refund, arguing that the rewards should be treated as newly created property (e.g. like ears of corn grown in a field) and therefore shouldn't be taxed until he sells them. The IRS denied that refund, and so he sued saying it was misinterpreting the law.

The lawsuit is still ongoing. However, as announced today by the Proof of Stake Alliance, the IRS may be trying to get out of it before they lose. They are now offering Josh his refund without admitting the merits of his argument.

Rightly, Josh is not taking the refund because he wants clear guidance from the IRS, not a mere monetary victory. So he hasn't won yet, but it does look like the IRS is realizing that their current policy may not be adequately justified by law, and may not survive a judgement from the court. That's great news.

Moreover, as we've previously written, this should not be interpreted as merely a positive development for proof of stake validators, it's good news for Bitcoin miners as well:

Any block reward from a permissionless cryptocurrency network, whether it is created through proof-of-work mining, proof-of-stake validating, or some other mechanism, is most accurately described as the creation of value through one's own capital and labor rather than the receipt of value from an employer. The network allows users to create wealth from their own resources, it does not pay people for their labor. Why is this the more sensible characterization? Creators of block rewards literally do not get paid by anyone. Who is the employer when you are working for the bitcoin network? Just as truly permissionless decentralized networks lack third party promoters upon whom users rely in the context of securities law, they also lack discernible employers and employees in the context of income tax law. To be clear, that does not mean that block rewards can or should be tax free, simply that they should be taxed like crops, minerals, livestock, artwork, and assembly line widgets: they should be taxed when they are sold, not when they are created.

Treating mining and staking rewards as newly created property rather than income is also the preferred approach of a bipartisan group in Congress who sent the IRS a letter arguing as much in August of 2020. Today's news brings us one step closer to winning that fight and one step closer to clear and reasonable tax policy for crypto in the US.

Open Blockchains and Decentralized Identity Standards

An open letter to the W3C Director, CEO, team, and membership

by Peter Van Valkenburgh September 28, 2021

Coin Center is the leading non-profit research and advocacy center focused on the public policy issues facing cryptocurrency and decentralized computing technologies. Our mission is to build a better understanding of these technologies and to promote a regulatory climate that preserves the freedom to innovate using permissionless blockchain technologies. We are not a member of the W3C but share a mutual desire to encourage the development of a freer, more open internet. We write today in response to recent objections by Mozilla and other major technology corporations to the Decentralized Identifiers (DIDs) proposed recommendation.

As we've previously written, "blockchain technology" is generally an overhyped buzzword. In truth, it is the open consensus mechanism of *some* blockchain networks, rather than the mere existence of a mythical "blockchain," that is the true innovation in our field. Additionally, only a few use cases actually benefit from that innovation: electronic cash (e.g. Bitcoin) chief among them. That said, one of the few genuine use cases for open blockchain networks beyond electronic cash is digital identity.

Like electronic cash, digital identity should be open: anyone should be able to create identifiers and issue identity credentials to anyone else without needing to adopt proprietary technologies and without seeking permission from a gatekeeper. Additionally, anyone should be able to build applications that can leverage portable and interoperable digital identity credentials without needing to buy access to an API or form an agreement with some dominant identity provider. As with electronic cash, an individual should be able to directly possess and control her own digital identity and should not need to rely upon some third party's ability and willingness to preserve the integrity and privacy of those identifiers and credentials. Only open blockchain networks can ultimately provide the openness and individual possession and control that a fair and well-functioning digital identity system would demand.

Today we have the complete opposite of that system. Current digital identity systems are closed: your identifiers come from a company (e.g. Twitter handle, Facebook name, domain name, telephone number, etc.) and your credentials are held captive at one or several siloed database providers (e.g. social networking sites, banks, credit rating agencies, or government agencies, etc.). One provider may not be willing to cooperate on standards with another provider, and a new business seeking to leverage established digital identities is at the mercy of the existing identity providers for interoperability and access. These systems do not allow for individual ownership and control over identifiers and credentials: when you are proving your identity to someone else online you are not

sharing a digital certificate over which you have actual cryptographic control, you are, instead, asking a middleman to share that credential on your behalf (e.g. sign-on with Google, sign-on with Facebook, etc.). Your privacy and the integrity of your data are wholly dependent on the quality of the cybersecurity practices of that middleman. Worse, when one of these middlemen is hacked, all of their user data is compromised in bulk (e.g. the Equifax hack).

With all that in mind, we are disappointed that a promising effort to standardize Decentralized Identifiers (DIDs) at the W3C is being waylaid by the objections of centralized digital identity providers. Those objections are, perhaps, unsurprising because they are coming from companies with the most to lose from a future, more open, digital identity landscape. However, the tone of these objections is particularly disappointing. Rather than critiquing the pending W3C DID standard on the merits, these objections have jumped to scare tactics and hyperbole.

The Mozilla objection, for example, dedicates the vast majority of its critique to the putative environmental costs of proof of work mining. This is transparently irrelevant to the W3C DID standardization process. Not only does the current DID standard never mention proof of work mining as essential to the proposed scheme, it doesn't even mention blockchains of any kind. While it is true that the current DID standard *can* be used in conjunction with open blockchain networks (and that is something worth celebrating for the reasons outlined above) it by no means requires blockchain networks for its functionality. Nor does the standard even remotely suggest that a proof of work blockchain specifically would be necessary. The DID standards could be implemented, for example, on proof of stake blockchains that do not utilize anywhere near as much energy in their consensus mechanism or they could be implemented without blockchains at all.

At the end of the day, the current standard simply provides options for future uses: if the larger internet community found any particular blockchain useful in implementing the DID standard then that choice could be made. But if, on the other hand, the environmental or other cost of implementing the DID standard using blockchains was prohibitive, then other methods could be used. The current standard does not lock anyone into any particulars. Indeed, it's confusing that this flexibility of methods is also something that the Mozilla objection criticizes. How can the standard both be too permissive of various methods (blockchain and non-blockchain) while simultaneously too deterministic in locking the community into a particular method that, it is alleged, would have deleterious environmental consequences?

Moreover, the energy usage of a proof of work blockchain, like Bitcoin's, could be entirely justified if it was leveraged to provide robust security for a global identity network. Energy usage alone does not inherently equate to environmental degradation. Developing clean energy sources and discouraging the burning of fossil fuels is a far wiser environmental policy goal than simply forgoing the potential benefits of increased energy consumption for important processes. The best of all worlds might be one where tremendous energy resources are dedicated to forging a secure and open identity standard that significantly

discourages hacking and fraud but where all of that energy comes from clean and renewable sources.

We urge the W3C to look closely at these objections. Do they critique the actual DID standard or do they instead critique a strawman?

Thank you,

Peter Van Valkenburgh

Coin Center Director of Research

Congress of the United States
Washington, DC 20515

July 29, 2020

The Honorable Charles P. Rettig
Commissioner
Internal Revenue Service
1111 Constitution Avenue, NW
Washington, DC 20224

CC:

The Honorable Michael J. Desmond
Chief Counsel
Internal Revenue Service
1111 Constitution Avenue, NW
Washington, DC 20224

The Honorable David J. Kautter
Assistant Secretary (Tax Policy)
Department of the Treasury
1500 Pennsylvania Avenue, NW
Washington, DC 20220

Dear Commissioner Rettig:

We write on the subject of blockchain and cryptocurrency – in particular the taxation of the newer variety known as “proof of stake.” It is important that tax policy does not indirectly dissuade U.S. taxpayers from participating in this promising new technology.

The Bitcoin network is secured by a relatively small number of “miners” who validate transactions as they “mine” new bitcoins. In “proof of stake”, in contrast, all tokenholders can contribute to network security by “staking” their tokens and so many, or even most, tokenholders end up holding newly created tokens. This means that network security in proof of stake does not require massive amounts of energy consumption.

These new tokens, often known as “block rewards,” incentivize people to maintain the network and are typically carried out through a third-party service (“staking as a service” provider). These third-parties work to simplify the technical processes and we believe that taxpayers’ true gains from these tokens should indeed be taxed. However, it is possible the taxation of “staking” rewards as income may overstate taxpayers’ actual gains from participating in this new technology. It could also result in a reporting and compliance nightmare, for taxpayers and the Service alike.

Those who help validate transactions create new blocks in the cryptocurrency blockchain and also create these new tokens. Similar to all other forms of taxpayer-created (or taxpayer-discovered) property – such as crops, minerals, livestock, artworks, and even widgets off the assembly line – these tokens could be taxed when they are sold.

American ingenuity can help drive this new technology. We thank you for considering our concerns as part of our continual efforts to future proof policy and tax regulations that will allow for safeguards, but also ensure that innovation won't be driven elsewhere.

Sincerely,



David Schweikert
Member of Congress



Bill Foster
Member of Congress



Tom Emmer
Member of Congress



Darren Soto
Member of Congress

TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION



The Internal Revenue Service Can Improve Taxpayer Compliance for Virtual Currency Transactions

September 24, 2020

Reference Number: 2020-30-066

TIGTACommunications@tigta.treas.gov | www.treasury.gov/tigta | 202-622-6500

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

Redaction Legend:

1=Tax Return/Return Information

2=Law Enforcement Techniques/Procedures and Guidelines for Law Enforcement Investigations or Prosecutions.

7=Information Reflecting the Bureau's Decisionmaking Process

To report fraud, waste, or abuse, please call us at 1-800-366-4484

HIGHLIGHTS: The Internal Revenue Service Can Improve Taxpayer Compliance for Virtual Currency Transactions



Final Audit Report issued on September 24, 2020
Reference Number 2020-30-066

Why TIGTA Did This Audit

This audit was initiated because the use of virtual currency as a payment method continues to grow in popularity and is emerging as an alternative asset to U.S. or other fiat currencies. This audit focuses on virtual currency exchanges because they play an important role in the transferability and stability of virtual currency by facilitating the buying and selling of virtual currencies for customers. The overall objective of this review was to evaluate the IRS's efforts to ensure the accurate reporting of virtual currency transactions as required under U.S. Code Titles 26 (Internal Revenue Code) and 31 (Money and Finance).

Impact on Taxpayers

The sale or exchange of virtual currencies, the use of virtual currencies to pay for goods or services, and holding virtual currencies as an investment generally have tax consequences that could result in tax liability. Taxpayers who do not properly report the income tax consequences of virtual currency transactions may be liable for tax, penalties, and interest. In addition to taxpayers' virtual currency transactions, the IRS reviews virtual currency exchanges, which engage in the business of exchanging virtual currency for fiat currency or other virtual currency. While exchanges are in a position to provide important information for use by the IRS in tax administration, information reporting on virtual currency transactions from the exchanges is lacking.

What TIGTA Found

TIGTA found that it is difficult for the IRS to identify taxpayers with virtual currency transactions because of the lack of third-party information reporting that specifically identifies virtual currency transactions. As of October 2018, both the Large Business and International and the Small Business/Self-Employed (SB/SE) Divisions' examination functions have started a small number of examinations of taxpayers based on potential virtual currency issues, and the SB/SE Division's examination function has few known open examinations of virtual currency exchanges.

TIGTA reviewed the examination case files for seven judgmentally sampled virtual currency exchange examinations closed by Bank Secrecy Act (BSA) Program examiners and found that some exchanges exhibited business characteristics that may qualify them as Third-Party Settlement Organizations (TPSOs) under Internal Revenue Code Section 6050W. This would require the filing of Form 1099-K, *Payment Card and Third Party Network Transactions*, for customers with more than 200 transactions in a year that total in excess of \$20,000. However, some of the exchanges that appeared to be TPSOs issued Forms 1099-K for Tax Years 2015 to 2018. Additionally, TIGTA reviewed the Form 1099-B, *Proceeds From Broker and Barter Exchange Transactions*, filing data for nine virtual currency exchanges for Tax Years 2015 to 2018 and was only able to identify **1** ****1**** that issued Forms 1099-B to its customers for that period.

Although BSA Program examiners generally pursue Title 31 issues, they are encouraged to make referrals to the BSA Examination Case Selection for Title 26 income tax examinations if they identify issues that indicate noncompliance. However, Title 31 examiners did not generally identify income tax issues and refer examinations to Title 26 examination groups. None of the examinations in TIGTA's review had potential Title 26 issues referred.

What TIGTA Recommended

TIGTA recommended that the IRS continue efforts to close the virtual currency information gap by issuing guidance clarifying the proper information reporting associated with virtual currency transactions. TIGTA also recommended that the IRS develop a process to use and monitor Title 31 virtual currency information in Title 26 examination workload.

IRS management agreed with both recommendations. The IRS stated that it is currently working with the Treasury Department to develop guidance on third-party reporting under Internal Revenue Code Section 6045 for certain taxable transactions involving virtual currency. The IRS also stated that an Interim Guidance Memo provides guidance and references a monitored process for a Title 26 examiner to use Title 31 information. In addition, the IRS stated that some Title 31 data was made available to the Title 26 program.



TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 24, 2020

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The Internal Revenue Service Can Improve
Taxpayer Compliance for Virtual Currency Transactions
(Audit # 201830034)

This report presents the results of our review to evaluate the Internal Revenue Service's efforts to ensure the accurate reporting of virtual currency transactions as required under U.S. Code Titles 26 and 31. This review is part of our Fiscal Year 2020 Annual Audit Plan and addresses the major management and performance challenge of *Improving Tax Reporting and Payment Compliance*.

Management's complete response to the draft report is included as Appendix II.

Copies of this report are also being sent to the Internal Revenue Service managers affected by the report recommendations. If you have any questions, please contact me or Matthew A. Weir, Assistant Inspector General for Audit (Compliance and Enforcement Operations).



The Internal Revenue Service Can Improve Taxpayer Compliance for Virtual Currency Transactions

Table of Contents

<u>Background</u>	Page 1
--------------------------------	--------

<u>Results of Review</u>	Page 5
---------------------------------------	--------

<u>Limited Guidance on Virtual Currency Information Reporting Obligations Impacts Tax Compliance</u>	Page 5
--	--------

<u>Recommendation 1:</u>	Page 10
--------------------------------	---------

<u>Few Title 26 Examinations Involving Virtual Currency Exchanges Were Conducted</u>	Page 10
--	---------

<u>Only a Small Number of Virtual Currency Exchange Examinations Were Conducted by the Small Business/Self-Employed Division's Bank Secrecy Act Program</u>	Page 12
---	---------

<u>Recommendation 2:</u>	Page.19
--------------------------------	---------

Appendices

<u>Appendix I – Detailed Objective, Scope, and Methodology</u>	Page 20
--	---------

<u>Appendix II – Management's Response to the Draft Report</u>	Page.22
--	---------

<u>Appendix III – Abbreviations</u>	Page.25
---	---------



The Internal Revenue Service Can Improve Taxpayer Compliance for Virtual Currency Transactions

Background

Virtual currency is a digital representation of value, other than a representation of the U.S. dollar or a foreign currency ("fiat" currencies), which functions as a unit of account, a store of value, and a medium of exchange.¹ Virtual currencies are stored in "virtual currency wallets" and can be digitally traded between users as well as be purchased for, or exchanged into, U.S. dollars, euros, and other fiat or virtual currencies through a direct peer-to-peer system.² Virtual currencies are often described as "cryptocurrencies" because they use cryptographic protocols to secure transactions recorded on publicly available decentralized ledgers, called "blockchains."³ Virtual currency that has an equivalent value in fiat currency, or that acts as a substitute for fiat currency, is referred to as "convertible" virtual currency. Bitcoin is one example of convertible virtual currency. Although the value of virtual currency has varied substantially in recent years, as of April 2020, there were over 5,000 virtual currencies with market capitalization exceeding \$214 billion, in addition to unreported virtual currency transactions.⁴

The use of virtual currency as a payment method continues to grow in popularity and is emerging as an alternative asset to U.S. or other fiat currencies.⁵ Making payments in virtual currency, instead of fiat currency, may allow users to pay lower transaction fees and achieve faster transfer of funds. However, the use of virtual currency may also allow anonymity in transactions and the possibility of avoiding tax reporting obligations. Taxation compliance risks can arise from willful conduct by a taxpayer (*e.g.*, using virtual currency to evade taxes) or nonwillful conduct (*e.g.*, lack of understanding of the taxability of virtual currency transactions, calculation of gain/loss from virtual currency transactions, characterization of income, third-party reporting responsibilities, *etc.*).

The Internal Revenue Service's (IRS) latest estimate of the gross Tax Gap, the amount of tax liability not paid voluntarily and timely, was \$441 billion annually for Tax Years (TY) 2011 through 2013. The gross Tax Gap is comprised of taxpayers who did not timely pay tax and timely file required returns (nonfiling), taxpayers misreporting amounts used to calculate tax liabilities on timely filed returns (underreporting), and taxpayers not paying tax liabilities reported on timely filed tax returns (underpayment). The IRS estimates that these components contribute, on average, \$39 billion, \$352 billion, and \$50 billion, respectively, to the gross Tax Gap annually.

This audit focuses on virtual currency exchanges because they play an important role in the transferability and stability of virtual currency by facilitating the buying and selling of virtual currencies for customers. Unlike U.S. currency, virtual currency is not legal tender that must be

¹ Fiat currency is the name for what is traditionally recognized as currency. Fiat currency is the coin and paper money of a country and designated as its legal tender.

² A "virtual currency wallet" is a means (software application or other mechanism/medium) for holding, storing, and transferring bitcoins or other virtual currency.

³ *Commodity Futures Trading Commission v. McDonnell*, 287 F.Supp.3d 213 (E.D. NY 2018).

⁴ CoinMarketCap, All Cryptocurrencies, available at <https://coinmarketcap.com/all/views/all/> (last visited Apr. 23, 2020). Cryptocurrencychart.com indicates price fluctuations of the top twenty five cryptocurrencies through the years 2010 to 2020.

⁵ IRS, Pub. 5316, *Internal Revenue Service Advisory Council Public Report November 2018* p. 72 (Nov. 2018).



The Internal Revenue Service Can Improve Taxpayer Compliance for Virtual Currency Transactions

accepted as payment.⁶ Virtual currency exchanges allow virtual currency to be readily exchanged for legal tender. While these exchanges are in a position to provide important information for use by the IRS in tax administration, information reporting on virtual currency transactions from the exchanges is lacking. The IRS's most recent Tax Gap study, issued in September 2019, found that noncompliance varies with the amount of information reporting by third parties (*e.g.*, employers, banks, partnerships). Items subject to substantial information reporting and withholding (*e.g.*, wages) have a net misreporting rate of 1 percent for the individual income tax. However, the net misreporting rate for items subject to some information reporting (*e.g.*, partnership income) is 17 percent, and the net misreporting rate for items subject to little or no information reporting (*e.g.*, nonfarm proprietor income) is 55 percent.

Tax consequences of virtual currency transactions

The sale or exchange of virtual currencies, the use of virtual currencies to pay for goods or services, and holding virtual currencies as an investment generally have tax consequences that could result in tax liability. In March 2014, the IRS issued Notice 2014-21 as guidance for individuals and businesses on the tax treatment of transactions using virtual currencies.⁷ According to Notice 2014-21, the general tax principles that apply to property transactions also apply to transactions using virtual currency. For example:

- A payment made using virtual currency is subject to information reporting to the same extent as any other payment made in property.
- A payment made using virtual currency made to independent contractors and other service providers is taxable, and self-employment tax rules generally apply. Normally, payers must issue Form 1099-MISC, *Miscellaneous Income*.
- Wages paid to an employee using virtual currency are taxable to the employee, must be reported by an employer on a Form W-2, *Wage and Tax Statement*, and are subject to Federal income tax withholding and payroll taxes.
- Virtual currency may be used to pay for goods or services. Certain third parties who settle payments made in virtual currency on behalf of merchants that accept virtual currency from their customers are required to report payments to those merchants on Form 1099-K, *Payment Card and Third Party Network Transactions*.
- The character of gain or loss from the sale or exchange of virtual currency depends on whether the virtual currency is a capital asset in the hands of the taxpayer.

In October 2019, the IRS issued Revenue Ruling 2019-24, which offered guidance on the income tax consequences of "airdrops" and "hard forks."⁸ The IRS also expanded upon the examples provided in Notice 2014-21 by providing a series of frequently asked questions on its website to assist taxpayer reporting of virtual currency tax matters.⁹ In another important initiative, the IRS

⁶ 31 United States Code (U.S.C.) Section (§) 5103.

⁷ IRS, IRS Notice 2014-21, *IRS Virtual Currency Guidance*; 2014-16 I.R.B. p. 938.

⁸ IRS, IRS Rev. Rul. 2019-24; 2019-44 I.R.B. p. 1004. An "air drop" involves the distribution of virtual currency to users, and a "hard fork" involves the splitting of a blockchain into incompatible versions of the currency.

⁹ IRS, *Frequently Asked Questions on Virtual Currency Transactions*, dated Dec. 2019, available at <https://www.irs.gov/individuals/international-taxpayers/frequently-asked-questions-on-virtual-currency-transactions> (last visited July 22, 2020).



The Internal Revenue Service Can Improve Taxpayer Compliance for Virtual Currency Transactions

created a question on Schedule 1, *Additional Income and Adjustments to Income*, for the TY 2019 Form 1040, *U.S. Individual Income Tax Return*, asking whether taxpayers have received, sold, sent, exchanged, or acquired an interest in virtual currency. If taxpayers answer truthfully, the question provides some information to the IRS about risks related to tax compliance coming from virtual currencies; however, the question does not require taxpayers to provide the nature and extent of such transactions that, if provided, would give the IRS a more complete understanding of tax compliance risk related to virtual currency transactions.

Taxpayers who do not properly report the income tax consequences of virtual currency transactions may be liable for tax, penalties, and interest. In some cases, taxpayers could be subject to criminal prosecution. In addition to taxpayers' virtual currency transactions, the IRS reviews virtual currency exchanges, which engage in the business of exchanging virtual currency for fiat currency or other virtual currency.

Federal oversight of virtual currencies

There is concurrent oversight involving virtual currencies among Federal agencies. The Commodity Futures Trading Commission has asserted jurisdiction over transactions involving virtual currencies, treating them as commodities.¹⁰ The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) has authority over money service businesses (MSBs) with reporting obligations under the Bank Secrecy Act (BSA).¹¹ FinCEN exercises regulatory functions primarily under the Currency and Foreign Transactions Reporting Act of 1970, as amended by other legislation, a legislative framework commonly referred to as the BSA.

Congress enacted the BSA in 1970 to fight money laundering and other financial crimes. The BSA authorizes the Secretary of the Treasury to issue regulations requiring banks and other financial institutions to take a number of precautions against financial crime, including the establishment of anti-money laundering programs and the filing of reports that have been determined to have a high degree of usefulness in criminal, tax, and regulatory investigations and proceedings and certain intelligence and counter-terrorism matters. Virtual currency exchanges are deemed MSBs under FinCEN regulations.¹²

The IRS oversees enforcement of the taxable implications of virtual currency transactions.¹³ The IRS's Large Business and International (LB&I) Division and Small Business/Self-Employed (SB/SE) Division jointly have responsibility for virtual currency tax compliance. In July 2018, the LB&I Division announced a Virtual Currency Compliance campaign led by its Withholding and International Individual Compliance practice area.¹⁴ The campaign aims to address

¹⁰ The Commodity Futures Trading Commission oversees "accounts, agreements ... and transactions involving swaps or contracts of sale of a commodity for future delivery..." 7 U.S.C. § 2. See also Government Accountability Office, *Virtual Currencies: Additional Information Reporting and Clarified Guidance Could Improve Tax Compliance* (Feb. 2020), and *Commodity Futures Trading Commission v. McDonnell*, 287 F. Supp. 3d 213 (E.D. NY 2018).

¹¹ Pub. L. No. 91-508, 84 Stat. 1114 to 11244 (1970) (codified as amended in scattered sections of 12 U.S.C., 15 U.S.C., and 31 U.S.C.). Regulations for the Bank Secrecy Act, and other related statutes, are 31 C.F.R. 103.11-103.77 (2010).

¹² FIN-2013-G001.

¹³ As described above, the IRS has issued one notice and one revenue ruling providing guidance on the taxation of virtual currencies.

¹⁴ The Withholding and International Individual Compliance practice area has responsibility for the following taxpayers: U.S. citizens living or working abroad or in a U.S. Territory, U.S. citizens or resident aliens who hold income-producing assets in a foreign country or claim the foreign earned income exclusion or foreign tax credit, and permanent residents and nonresident aliens who have a U.S. filing requirement.



The Internal Revenue Service Can Improve Taxpayer Compliance for Virtual Currency Transactions

noncompliance related to the use of virtual currency through multiple treatment streams, including outreach and examinations. The intended compliance outcomes of the LB&I Division's Virtual Currency Compliance campaign include:

- Identify causes of noncompliance through a feedback loop and examination results.
- Identify additional treatment streams to increase compliance and reduce taxpayer burden.
- Improve examiner knowledge and skills as related to virtual currency transactions.
- Assist in developing a comprehensive IRS virtual currency strategy.

The LB&I Division's Virtual Currency Compliance campaign includes approved treatment streams such as soft letter(s), issue-based examinations, external events, and outreach. The Campaign has implemented virtual currency examination field work through third-party information reports.

The SB/SE Division has two different examination functions that may encounter virtual currency issues during examinations. The SB/SE Division's Specialty Examination function maintains a BSA Program, which conducts reviews under Title 31 (Money and Finance) of the United States Code (U.S.C.) as well as under provisions of U.S.C. Title 26 (Internal Revenue Code (I.R.C.) Section (§) 6050I).¹⁵ FinCEN has delegated responsibility for Title 31 compliance to the BSA Program.

The SB/SE Division's Field Examination program conducts taxpayer audits under Title 26 of the U.S.C. (Internal Revenue Code). The BSA Program, with only 237 full-time equivalents in Fiscal Year (FY) 2017, is significantly smaller than the SB/SE Division's Field Examination function, with 5,225 full-time equivalents.¹⁶

In a September 2018 report, we found that, for FYs 2014 through 2016, the BSA Program had estimated labor expenses of approximately \$97 million, which resulted in assessing only \$39 million in BSA-related penalties.¹⁷ We also found that systemic delays associated with the FinCEN penalty referral process resulted in only 80 cases referred to FinCEN and six penalties assessed by FinCEN from 24,212 BSA cases worked for FYs 2014 through 2016 and that the BSA Program's Title 31 compliance reviews appeared to be having little impact because of the IRS's lack of penalty authority.¹⁸ Our report made five recommendations, including that the IRS coordinate with FinCEN on the authority to assert Title 31 penalties or reprioritize resources to more productive work. The IRS did not agree with this recommendation, stating that the action was outside its purview and FinCEN intended to retain this authority. The Acting Inspector General of the Treasury, with oversight authority over FinCEN, made an observation similar to TIGTA's September 2018 report finding about Title 31 penalty authority in testimony at a 2004 hearing on money laundering and terrorism financing by stating that an October 2002 audit

¹⁵ I.R.C. § 6050I requires that any person engaged in a trade or business that receives in the course of such trade or business more than \$10,000 in cash must make a report to the Government as required by the statute.

¹⁶ Full-time equivalent is the total number of regular straight-time hours (*i.e.*, not including overtime or holiday hours) worked by employees divided by the number of paid hours applicable to each fiscal year. Annual leave, sick leave, compensatory time off, and other approved leave categories are considered to be "hours worked" for purposes of defining full-time equivalent employment. Full-time equivalent figures reported in IRS SB/SE Division, Small Business/Self-Employed Business Performance Review, 4th Quarter FY 2017 (Nov. 2017).

¹⁷ TIGTA, Ref. No. 2018-30-071, *The Internal Revenue Service's Bank Secrecy Act Program Has Minimal Impact on Compliance* (Sept. 2018).

¹⁸ The penalty related to the Report of Foreign Bank and Financial Accounts under 31 U.S.C. § 5314 is the only Title 31 penalty for which assessment authority has been delegated to the IRS.



The Internal Revenue Service Can Improve Taxpayer Compliance for Virtual Currency Transactions

found that FinCEN was inconsistent and untimely in its enforcement actions against casinos for BSA violations referred by the IRS.¹⁹ The testimony expressed the concern that the IRS might be reluctant to refer future casino BSA violations to FinCEN.

The Government Accountability Office (GAO) recently reviewed the IRS's efforts to ensure compliance with tax obligations for virtual currencies.²⁰ The GAO found that the IRS has limited data on tax compliance for virtual currencies because of limited information reporting by third parties, such as financial institutions. The GAO also found that many virtual currency transactions likely go unreported to the IRS, due in part to unclear requirements and thresholds that limit the number of virtual currency users subject to third-party reporting.

Results of Review

Due to limited information reporting that specifically identifies virtual currency transactions, the IRS cannot easily identify taxpayers with virtual currency transactions. In addition, few examinations of virtual currency exchanges are conducted by either Title 26 Field Examination groups or Title 31 BSA Program examination groups.

Limited Guidance on Virtual Currency Information Reporting Obligations Impacts Tax Compliance

Tax compliance is higher when there is third-party information reporting provided to the IRS on income earned with respect to a taxpayer. The IRS estimates that tax compliance is approximately 95 percent when there is substantial information reporting, and when there is substantial information reporting combined with tax withholding, tax compliance is estimated to be 99 percent.²¹ However, tax compliance drops to 45 percent when there is little or no information reporting or withholding.

Currently, there is an information reporting gap for virtual currency transactions.

Currently, there is an information reporting gap for virtual currency transactions because many such transactions are not reported to the IRS, and the transactions that are reported are not reported specifically as virtual currency transactions. Under existing IRS guidance, some virtual currency transactions are required to be reported in certain situations. However, there are two essential problems with virtual currency transaction reporting.

First, as the Treasury Inspector General for Tax Administration (TIGTA) reported in September 2016, third-party reporting of taxable transactions to the IRS does not separately identify transactions related to virtual currency.²² Employers and businesses are required to report taxable virtual currency transactions on information reporting documents such as

¹⁹ *Money Laundering and Terrorism Financing, Hearing Before the H. Comm. on Financial Services*, 108th Cong. (2004) (statement of Dennis S. Schindel, Acting Inspector General, Department of Treasury).

²⁰ GAO, GAO-20-188, *Virtual Currencies: Additional Information Reporting and Clarified Guidance Could Improve Tax Compliance* (Feb. 2020).

²¹ IRS, Pub. 1415, *Federal Tax Compliance Research: Tax Gap Estimates for Tax Years 2011–2013* (2019).

²² TIGTA, Ref. No. 2016-30-083, *As the Use of Virtual Currencies in Taxable Transactions Becomes More Common, Additional Actions Are Needed to Ensure Taxpayer Compliance* (Sept. 2016).



The Internal Revenue Service Can Improve Taxpayer Compliance for Virtual Currency Transactions

Form W-2 (when virtual currency is paid to employees), Form 1099-MISC (generally when virtual currency is paid of \$600 or more in settlement of services provided by an entity in a trade or business), and Form 1099-K (which will be described more fully below). However, these information returns currently do not provide any specific way to identify that the taxable transaction amounts being reported are related to virtual currencies. TIGTA recommended in its September 2016 report that the IRS's Deputy Commissioner for Services and Enforcement should revise third-party information reporting documents to identify the amounts of virtual currency used in taxable transactions. The IRS agreed with TIGTA's recommendation but stated that modifying information reporting documents to capture virtual currency amounts was not a priority for the IRS.

Second, as we describe in more detail below, while there is clarity that Form 1099-K must be provided to the IRS for certain limited virtual currency transactions, the information reporting requirements do not apply to all virtual currency exchanges. Another information reporting form, Form 1099-B, *Proceeds from Broker and Barter Exchange Transactions* (which is required to be filed for broker-related transactions), may be available to report virtual currency transactions. As discussed later in this report, the IRS and Department of the Treasury are currently considering whether to issue guidance relating to reporting virtual currency transactions under I.R.C. § 6045, which governs information reporting by brokers.

Not all virtual currency exchanges are required to report transactions on Form 1099-K

I.R.C. § 6050W requires reporting of certain payments made in settlement of payment card and third-party network transactions.²³ A "third-party payment network" is any agreement or arrangement that:

- Involves the establishment of accounts with a central organization by a substantial number of persons (*e.g.*, more than 50) who are unrelated to such organization, provide goods or services, and have agreed to settle transactions for the provision of such goods or services pursuant to such agreement or arrangement.
- Provides for standards and mechanisms for settling such transactions.
- Guarantees persons providing goods or services pursuant to such agreement or arrangement that such person will be paid for providing such goods or services.

I.R.C. § 6050W requires any "payor," or payment settlement entity, making one or more payments to a participating payee in settlement of "reportable payment transactions" to file Form 1099-K annually with the IRS. The payor reports the gross amount of such reportable payment transactions for the calendar year and for each month within such calendar year. The payor must also report the name, address, and Taxpayer Identification Number of the participating payees on Form 1099-K.²⁴

Virtual currency exchanges may be considered third-party settlement organizations (TPSOs) to the extent they settle payments made in virtual currency on behalf of merchants that accept virtual currency. A TPSO is a central organization that has a contractual obligation to make

²³ I.R.C. § 6050W requires payment settlement entities to issue Form 1099-K statements to payees who meet the criteria of I.R.C. § 6050W(e). Section 3091 of the Housing and Economic Recovery Act of 2008 (Pub. L. 110-289) added I.R.C. § 6050W.

²⁴ A nine-digit number assigned to taxpayers for identification purposes. Depending upon the nature of the taxpayer, the Taxpayer Identification Number is an Employer Identification Number, a Social Security Number, or an Individual Taxpayer Identification Number.



The Internal Revenue Service Can Improve Taxpayer Compliance for Virtual Currency Transactions

payments to participating payees (generally, a merchant or business) in a third-party payment network.

Under the reporting requirements, the TPSOs must report the gross reportable transactions of the businesses to which they make payments provided the payee satisfies certain transaction volume and dollar thresholds. In general, the TPSOs are required to file Form 1099-K when the gross amount of total reportable payment transactions exceeds \$20,000 and the total number of such transactions exceeds 200 for the calendar year.²⁵ IRS guidance provides that certain third parties who settle payments made in virtual currency on behalf of merchants that accept virtual currency from their customers are required to report payments to those merchants on Form 1099-K.²⁶ IRS officials told us that it is unclear under the current rules whether virtual currency that is exchanged for fiat currency (or for another type of virtual currency) would be considered “goods or services” under the reporting rules of I.R.C. § 6050W. Our review of Form 1099-K filings by a judgmental sample of virtual currency exchanges in Figure 1 shows that these exchanges may be taking inconsistent positions from one another on information reporting requirements.²⁷ Figure 1 below shows that only four of these exchanges issued any Forms 1099-K in TYs 2015 to 2018, despite most having 30-day exchange volumes ranging from hundreds of millions to billions of dollars.

**Figure 1: Forms 1099-K Filed for Virtual Currency Exchanges
TYs 2015 to 2018**

	30-Day Exchange Volume ²⁸	Number of Forms 1099-K Issued			
		TY 2015	TY 2016	TY 2017	TY 2018
Exchange A	**1* ²⁹	78	41	11,298	7,416
Exchange B	**1**	0	0	0	0
Exchange C	**1**	0	0	0	0
Exchange D	**1**	0	0	0	0
Exchange E	**1**	0	0	0	0
Exchange F	**1**	14	76	1,437	940
Exchange G	**1**	0	0	0	0
Exchange H	**1**	0	0	0	1
Exchange I	Not on Top 100 Lists	0	0	210	0

Source: TIGTA analysis of IRS Form 1099-K filing data.

The BSA Program examines certain MSBs, as well as other businesses, for compliance with the BSA (U.S.C. Title 31), which requires that certain transactions be reported, as well as I.R.C. § 6050I

²⁵ I.R.C. § 6050W.

²⁶ IR-2018-71, March 23, 2018.

²⁷ A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

²⁸ Exchange volume from <https://coinmarketcap.com/rankings/exchanges>, as of January 13, 2020.

²⁹ This exchange volume represents a minimum amount based on a subsidiary of a parent company.



The Internal Revenue Service Can Improve Taxpayer Compliance for Virtual Currency Transactions

(U.S.C. Title 26). However, examining virtual currency exchanges has made up a small part of the BSA Program's work plan, as we describe further below.

We reviewed the examination case files for seven judgmentally sampled virtual currency exchange examinations closed by BSA Program examiners and found that three exchanges exhibited business characteristics that may qualify them as TPSOs under I.R.C. § 6050W, which would require the filing of Form 1099-K for customers with more than 200 transactions in a year that total in excess of \$20,000. We reviewed the contents of the seven Title 31 case files, including examination results, summaries, notes, and any attached information, to assess whether an exchange exhibited the characteristics or activity of a TPSO. The case files for three exchanges showed the following characteristics of a TPSO as outlined in I.R.C. § 6050W:

- The existence of a central organization with whom a substantial number of persons providing goods and services (who are unrelated to the central organization) have established accounts.
- An agreement between the central organization and the persons to settle transactions for the provision of goods or services.
- The establishment of standards and mechanisms for settling such transactions.
- The guarantee of payment in settlement of such transactions.

*****1*****
*****1*****
*****1*****
*****1*****
*****1***** According to these exchanges, they have been active in over 100 countries, with 1 million to over 30 million customers, and have exchanged more than \$4 billion to over \$150 billion in transactions.

We also researched other large exchanges not included in our sample that were based in the United States and exchanged virtual currency for U.S. fiat currency. We found *****1***** had issued Forms 1099-K in at least one of the years between TYs 2015 to 2018. The **1**
*****1*****
*****1*****

The IRS should require virtual currency exchanges to file Form 1099-B to disclose virtual currency transactions

Brokers are required to file Form 1099-B with the IRS to report transactions on behalf of customers. Form 1099-B instructions define brokers as "any person who, in the ordinary course of a trade or business, stands ready to effect sales to be made by others."³⁰ Brokers who sell commodities are included in the requirement to issue Forms 1099-B to customers.³¹

³⁰ IRS, 2020 Instructions for Form 1099-B, *Proceeds From Broker and Barter Exchange Transactions* (Nov. 18, 2019), available at <http://www.irs.gov/pub/irs-pdf/i1099b.pdf>.

³¹ The I.R.C. § 6045(g)(3)(B)(iii) definition of specified security includes a commodity, thereby requiring commodity brokers to issue Form 1099-B to customers for commodity transactions. Commodities are subject to Form 1099-B reporting due to the application of Treas. Reg. § 1.6045-1(c)(1) (brokers must report on "sales") and Treas. Reg. § 1.6045-1(a)(9) (definition of "sales" includes disposition of commodities).



The Internal Revenue Service Can Improve Taxpayer Compliance for Virtual Currency Transactions

At least one Federal court has held that virtual currencies are “commodities” for purposes of being subject to Commodity Futures Trading Commission regulations. In *Commodity Futures Trading Commission v. McDonnell*, the U.S. District Court for the Eastern District of New York noted that commentators argue: “Bitcoin should primarily be considered a commodity because it serves the function of money in its community of users.”³² One legal commentator has opined that virtual currency exchanges are already required to file Form 1099-B, while one executive of a virtual currency exchange suggested that rather than having the IRS serve John Doe Summons to obtain client information, the IRS should just require exchanges to file Forms 1099-B.³³

The GAO’s February 2020 report stated that the IRS does not have an official position about whether virtual currency exchanges are required to report customer trading activity on Form 1099-B. The GAO also reported that it was only able to identify one exchange that stated that it reports customers’ transactions on Form 1099-B. TIGTA reviewed Form 1099-B filing data for the nine virtual currency exchanges in Figure 1 for TYs 2015 to 2018. As shown in Figure 2 below, we were also only able to identify one exchange that issued Forms 1099-B to its customers for that period.

**Figure 2: Forms 1099-B Filed for Virtual Currency Exchanges
TYs 2015 to 2018**

	30-Day Exchange Volume	Number of Forms 1099-B Issued			
		TY 2015	TY 2016	TY 2017	TY 2018
Exchange A	**1** ³⁴	0	0	0	0
Exchange B	**1**	0	0	0	0
Exchange C	**1**	0	0	0	0
Exchange D	**1**	0	0	0	0
Exchange E	**1**	0	0	0	0
Exchange F	**1**	0	0	0	0
Exchange G	**1**	103,414	194,532	412,720	642,402
Exchange H	**1**	0	0	0	0
Exchange I	Not on Top 100 Lists	0	0	0	0

Source: TIGTA analysis of IRS Form 1099-B filing data.

The 2019–2020 Priority Guidance Plan issued by the Department of the Treasury and the IRS in October 2019 includes “Guidance regarding information reporting on virtual currency under

³² *Commodity Futures Trading Commission v. McDonnell*, 287 F. Supp. 3d 213 (E.D. NY 2018), holding that Commodity Futures Trading Commission had jurisdiction over virtual currencies for purposes of issuing injunction to virtual currency exchange.

³³ *Digital Money: Bitcoin’s Financial and Tax Future Despite Regulatory Uncertainty*, 64 DePaul L. Rev. 213, 242 (2014). *Bitcoin: Breaking Bad or Breaking Barriers?*, 18 N.C. J.L. & Tech. On. 244, 255-256 (2017). There are times when the IRS must investigate violations, or potential violations, of Internal Revenue law by a person, group, or class of persons without identifying a specific individual. A John Doe summons is a summons that does not identify the person with respect to whose liability the summons is issued. Internal Revenue Manual 25.5.7.1.1 (June 4, 2020). I.R.C. § 7609(f) governs the requirements of an IRS-issued John Doe summons.

³⁴ This exchange volume represents a minimum amount based on a subsidiary of a parent company.



The Internal Revenue Service Can Improve Taxpayer Compliance for Virtual Currency Transactions

Section 6045” under the area of Tax Administration. I.R.C. § 6045 currently addresses reporting of securities, commodities, and other property but not specifically virtual currency. Based on TIGTA’s discussion with IRS Counsel, any future virtual currency guidance pertaining to I.R.C. § 6045 will address the types of third-party information reporting documents the exchanges should be issuing. *****2*****

*****2***** In our discussion, IRS

Counsel agreed that forms allowing taxpayers to identify virtual currency transactions would be beneficial.

The IRS cannot easily identify taxpayers with virtual currency transactions because of the lack of third-party information reporting that specifically identifies virtual currency transactions. An information reporting regime that requires all virtual currency exchanges to report all virtual currency transactions to the IRS would benefit tax compliance by closing the information gap with respect to virtual currencies.

Recommendation 1: The Deputy Commissioner for Services and Enforcement should continue efforts to close the virtual currency information gap by issuing guidance clarifying the proper information reporting associated with virtual currency transactions.

Management’s Response: The IRS agreed with this recommendation. In its response, the IRS stated that it is currently working with the Department of the Treasury to develop guidance on third-party reporting under I.R.C. § 6045 for certain taxable transactions involving virtual currency.

Few Title 26 Examinations Involving Virtual Currency Exchanges Were Conducted

As of October 2018, both the LB&I and SB/SE Divisions’ Examination functions started a small number of examinations of taxpayers based on potential virtual currency issues. These taxpayers were primarily identified from external information. These are considered to be pilot examinations that may help form policies, procedures, and processes for obtaining virtual currency data and performing examinations.

As of October 2018, both the LB&I and SB/SE Divisions’ Examination functions have started a small number of examinations of taxpayers based on potential virtual currency issues.

The IRS issued a “John Doe” summons in 2016 on Coinbase Inc., a virtual currency exchange headquartered in San Francisco, California. According to the summons, at the time, Coinbase offered buy and sell trading functionality in 33 countries, with 5.9 million customers served and \$6 billion in virtual currency exchanged. In November 2016, a Federal court in the Northern District of California authorized the IRS to file a John Doe summons on Coinbase for information on U.S. taxpayers who conducted transactions in a convertible virtual currency during Calendar Years 2013 to 2015. Coinbase failed to comply with the summons, and in March 2017, the IRS filed a petition to enforce the summons issued to Coinbase.³⁵

³⁵ *United States of America v. Coinbase Inc.*, Declaration of David Utzke in Support of Petition to Enforce Internal Revenue Summons, Case 3:17-cv-01431-JSC (N.D. Cal.).



The Internal Revenue Service Can Improve Taxpayer Compliance for Virtual Currency Transactions

To support the John Doe summons, the IRS analyzed electronically filed Forms 8949, *Sales and Other Dispositions of Capital Assets*, from the Modernized Tax Return Database for TYs 2013 through 2015.³⁶ The analysis indicated that only a small number of Forms 8949 included reports of property descriptions that were likely related to Bitcoin each year. For example, almost 129 million returns were electronically filed for TY 2015, and the IRS's search for Form 8949 data identified only 802 individuals who reported a transaction using a property description likely related to Bitcoin for that tax year.

Other than its involvement in LB&I Division's examinations, SB/SE Division's Field Examination function has few known open examinations of virtual currency exchanges. In 2018, the LB&I Division announced a Virtual Currency Compliance campaign with the objective of addressing noncompliance related to the use of virtual currency through multiple treatment streams, including outreach and examinations. The LB&I Division's Virtual Currency Compliance campaign announcement urged taxpayers with unreported virtual currency transactions to correct their returns as soon as practical because it is not contemplating a voluntary disclosure program specifically to address noncompliance involving virtual currency.

In July 2019, the IRS began sending educational letters to more than 10,000 taxpayers with virtual currency transactions that potentially failed to report income and pay the resulting tax from virtual currency transactions or did not report their transactions properly. The stated purpose of the mailings was to help taxpayers understand their tax and filing obligations and how to correct past errors. The following three variations of letters were mailed to the taxpayers: Letter 6173, *Virtual Currency Soft Notice*; Letter 6174, *Virtual Currency Education*; and Letter 6174-A, *Virtual Currency Education-Plus*.

- Letter 6173 required a response from the taxpayer. If the taxpayer does not timely respond, the IRS may consider an audit of the taxpayer.
- Letters 6174 and 6174-A do not require a response; however, an LB&I Director of Field Operations noted that the IRS still conducts risk assessments at that level and does not rule out auditing a taxpayer.³⁷

Regarding the letters, IRS Commissioner Chuck Rettig stated:

*Taxpayers should take these letters very seriously by reviewing their tax filings and, when appropriate, amend past returns and pay back taxes, interest, and penalties. The IRS is expanding our efforts involving virtual currency, including increased use of data analytics. We are focused on enforcing the law and helping taxpayers fully understand and meet their obligations.*³⁸

The SB/SE Division has conducted only a small number of Title 26 examinations of virtual currency exchanges

During our review, SB/SE Division officials informed us that, as of October 2018, they were not able to identify any known open Title 26 examinations of virtual currency exchanges. Therefore, we selected a judgmental sample of eight U.S.-based virtual currency exchanges that use U.S. fiat currency as a form of exchange to determine if any Title 26 examinations had been

³⁶ The Modernized Tax Return Database is the legal repository for original electronically filed returns received by the IRS through the Modernized e-File system.

³⁷ Andrew Velarde, "Taxpayers Can Expect More Virtual Currency Compliance Letters," Tax Notes Today, Oct. 23, 2019.

³⁸ IR-2019-132, July 26, 2019.



The Internal Revenue Service Can Improve Taxpayer Compliance for Virtual Currency Transactions

conducted on these exchanges from FYs 2015 to 2019. Figure 3 shows the names, number of markets, and 30-day transaction volume for the U.S.-based exchanges that we selected for our review.

Figure 3: U.S.-Based Virtual Currency Exchanges Selected for TIGTA's Review of Title 26 Examination Activity

Exchange	Number of Markets	30-Day Transaction Volume
Exchange A ³⁹	*1*	***1***
Exchange B	*1*	***1***
Exchange C	*1*	***1***
Exchange D	*1*	***1***
Exchange E	*1*	***1***
Exchange F	*1*	***1***
Exchange G	*1*	***1***
Exchange H	*1*	***1***

Source: <https://coinmarketcap.com/rankings/exchanges/> (last visited Jan. 13, 2020).

We researched these exchanges in the IRS's Audit Information Management System to determine if the IRS has conducted any Title 26 examinations on these exchanges from FY 2015 to FY 2019.⁴⁰ We found that examinations were selected for three of the eight exchanges in this five-year period. However, for these three exchanges as of the first quarter of FY 2020, *1*

*****1*****
*****1*****

Only a Small Number of Virtual Currency Exchange Examinations Were Conducted by the Small Business/Self-Employed Division's Bank Secrecy Act Program

The BSA requires that financial institutions retain records and file reports on transactions above certain thresholds as well as report suspicious activities. These reports are submitted to FinCEN, which collects and analyzes the information to support law enforcement investigative efforts and provide U.S. policy makers with strategic analyses of domestic worldwide money laundering developments, trends, and patterns. The BSA's reporting and recordkeeping provisions apply to banks, savings and loans, and credit unions as well as other financial institutions, including the MSBs, which can include convenience stores that enable customers to purchase money orders as well as other businesses that engage in similar services.

³⁹ The number of markets and the exchange volume represent a minimum amount based on a subsidiary of a parent company.

⁴⁰ The Audit Information Management System is an inventory of IRS examination cases; the system traces examination results through final determination of tax liability including Appeals and Tax Court.



The Internal Revenue Service Can Improve Taxpayer Compliance for Virtual Currency Transactions

The SB/SE Division's BSA Program examines whether these financial institutions, including the MSBs, are complying with reporting and recordkeeping provisions. The compliance requirements of the BSA include:

- Registering with FinCEN as an MSB.
- Preparing, implementing, and maintaining a written Anti-Money Laundering compliance program.
- Filing BSA reports, including Suspicious Activity Reports and Currency Transaction Reports.
- Maintaining records for certain types of transactions.
- Obtaining customer identification information sufficient to comply with Anti-Money Laundering requirements.

Additionally, a virtual currency transmitter that is a U.S. person must comply with all U.S. Treasury Office of Foreign Assets Control financial sanctions obligations.

In a February 2018 response to a letter from U.S. Senator Ron Wyden inquiring about FinCEN's virtual currency oversight, FinCEN stated that virtual currency exchanges must register as MSBs. The letter reiterated that virtual currency exchanges have been subject to the BSA since 2011. The letter stated that, as of February 2018, approximately one-third of the 100 virtual currency exchanges have been examined by FinCEN since 2014 in cooperation with the SB/SE Division.

A FinCEN Advisory states that foreign virtual currency exchanges doing business in the United States must register as MSBs with FinCEN.⁴¹ FinCEN noted that some foreign virtual currency exchanges purposely seek to operate outside of the United States to avoid U.S. regulatory oversight in favor of jurisdictions that lack or have limited anti-money laundering/countering the financing of terrorism controls. In addition, global collaboration between 37 countries takes place through the Financial Action Task Force, an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions. Its objectives are to set standards and promote effective implementation of legal, regulatory, and operational measures for combating money laundering, terrorist financing, and other related threats to the integrity of the international financial system.

In June 2019, the Financial Action Task Force issued new requirements for virtual currency exchanges to share customer information with one another when transferring funds. According to the U.S. Secretary of the Treasury, virtual currency exchanges will be required under the new guidance to implement the same anti-money laundering/countering the financing of terrorism requirements as traditional financial institutions. Virtual currency exchanges will be required to:

- Identify who they are sending funds on behalf of, and who is the recipient of those funds.
- Develop processes whereby they are required to share that information with other providers of virtual assets and law enforcement.
- Know their customers and conduct proper due diligence to ensure that they are not engaging in illicit activity.

⁴¹ Advisory FIN-2019-A003.



The Internal Revenue Service Can Improve Taxpayer Compliance for Virtual Currency Transactions

- Develop risk-based programs that account for the risks in their particular type of business.

In addition, the Financial Action Task Force requires participating countries to:

- Assess and mitigate the risks associated with virtual asset activities and service providers.
- License or register service providers and subject them to supervision or monitoring by competent national authorities and implement sanctions and other enforcement measures when service providers fail to comply with their (anti-money laundering/countering the financing of terrorism) obligations.
- Underscore the importance of international cooperation.

According to the Financial Action Task Force, some countries may decide to prohibit virtual asset activities based on their own assessment of the risks and regulatory context or to support other policy goals.

The SB/SE Division's BSA Program organizes its work plans under Title 31 and Form 8300 Examinations.⁴² The BSA Examination Case Selection function uses the Title 31 Non-Bank Financial Institution database to monitor virtual currency examinations. The BSA Examination Case Selection function is responsible for delivering an inventory of Non-Bank Financial Institutions subject to the BSA and regulations for which the IRS has been delegated authority to examine. The types of sources used to identify Non-Bank Financial Institutions include:

- External databases.
- Field referrals (referrals may require a related statute determination).
- BSA examiner referrals resulting from physical observation or review of competitor listings.
- FinCEN Query results.
- Neighborhood publications.
- Trade or business associations.
- IRS Research, Applied Analytics, and Statistics.
- BSA Compliance Department, Detroit special reports.
- Internet research.
- State and local licensing and/or regulatory agencies.
- Criminal Investigation referrals.
- MSB agent lists received from examiners and FinCEN.
- FinCEN referrals.
- Referrals from Federal, State, or local law enforcement agencies.

However, as of October 2018, BSA Policy officials were not aware of any policies or procedures for obtaining third-party information reporting on U.S. taxpayers from foreign-based exchanges.

⁴² The IRS has the authority to examine nonfinancial trades and businesses for compliance with the reporting requirements for Form 8300, *Report of Cash Payments Over \$10,000 Received in a Trade or Business*, under Titles 26 and 31.



The Internal Revenue Service Can Improve Taxpayer Compliance for Virtual Currency Transactions

According to the IRS, one of the primary data sources used to identify virtual currency examination leads for the BSA Program is a list of possible exchanges for examination and information received from FinCEN. The IRS noted that the BSA Program has started using external vendors who provide blockchain analytic tools to develop techniques to identify virtual currency exchanges. The IRS informed us that the BSA Program is also working with IRS Research, Applied Analytics, and Statistics staff to implement data staging and analytics for all BSA workstreams, including virtual currency.

Since FY 2016, the Title 31 program workstreams have included virtual currency examinations, including virtual currency exchanges. However, the bulk of Title 31 examination work for FY 2019 and FY 2020 consists of noncentralized small MSBs, although the SB/SE Division included some virtual currency exchanges in its FY 2019 examination plan.****2****

*****2*****7*****
*****2*****7*****

*****2*****7***** The FY 2020 Title 31 examination plan included 49 planned virtual currency examination starts and 34 planned virtual currency examination closures. However, as shown in Figure 4, virtual currency examinations make up less than 1 percent (12 of 3,392) of planned Title 31 examination closures for FY 2019 and slightly over 1 percent (34 of 3,063) for FY 2020 planned closures.

*****2*****
*****2*****

*****2*****	***2*** ***2*** ***2***	***2*** ***2*** ***2***	***2*** ***2*** ***2***	***2*** ***2*** ***2***43
*****2*****	**2**	**2**	**2**	**2**
*****2*****	**2**	**2**	**2**	**2**
*****2*****	**2**	**2**	**2**	**2**
*****2*****	**2**	**2**	**2**	**2**
*****2*****	**2**	**2**	**2**	**2**
*****2*****	**2**	**2**	**2**	**2**
*****2*****	**2**	**2**	**2**	**2**
*****2*****	**2**	**2**	**2**	**2**
*****2*****	**2**	**2**	**2**	**2**
*****2*****	**2**	**2**	**2**	**2**
*****2*****	**2**	**2**	**2**	**2**
*****2*****	**2**	**2**	**2**	**2**

*****2*****

⁴³ FY 2020 Closures to Date as of June 18, 2020.



The Internal Revenue Service Can Improve Taxpayer Compliance for Virtual Currency Transactions

In September 2018, TIGTA issued a report evaluating the impact of IRS's compliance efforts related to its delegated authority under the BSA. One of the recommendations was that the IRS leverage the BSA Program's Title 31 examination authority by incorporating its annual examination planning into the IRS's overall virtual currency strategy. The IRS agreed with the recommendation and is in the process of making virtual currency exchange examinations a significant part of its Title 31 examination plan. IRS management indicated that measuring closures by themselves does not reflect the resources applied to an emerging area such as virtual currency. The challenges of expending resources and time to introduce a new workstream, such as virtual currency, include:

- Workload identification and delivery.
- Training of examiners, including developing training materials, delivering classroom training, and on-the-job training with instructors.
- Balancing competing priorities and completing existing examination inventories.
- External factors, such as COVID-19, which impact potential closure of cases from examination groups.

The SB/SE Division has trained additional examiners to increase its examination coverage

As previously stated, TIGTA reviewed seven Title 31 examinations of virtual currency exchanges that were closed between December 2017 and February 2019 to evaluate the BSA Program's Title 31 compliance efforts and whether any referrals were made to the Title 26 examination function as a result of a Title 31 examination. The seven examinations averaged 187 examiner hours per case and generally covered an exam period of 180 days. Five of the seven examinations we reviewed were conducted by examiners at the General Schedule (GS) 13 level, and two examinations were conducted by an examiner at the GS-12 level or lower but with assistance from another examiner. According to IRS officials, the SB/SE Division BSA Program, in consultation with FinCEN, created virtual currency training and trained 18 examiners and managers in FY 2018 and 25 examiners and managers in FY 2019. As of June 2020, the SB/SE Division BSA Program has 64 virtual currency examinations open, which reflects increased resources directed at this high-risk industry.

When no BSA violations are found, the examiner issues the closing Letter 4029, *Bank Secrecy Act No Change Letter*. Letter 4029 states that no violations were identified during the examination period based on the scope and depth of the examination and the evaluation and testing of the implementation of the exchange's anti-money laundering compliance program. One case in our review reported no violations, one case was closed as a survey (no contact with the taxpayer), and five cases were closed with violations found.

Letter 1112, *Title 31 Violation Notification Letter*, is issued to the exchange if BSA violations are found, regardless if such violations meet the criteria for referral to FinCEN under the Internal Revenue Manual (IRM) referral guidelines. FinCEN also gets courtesy copies of all Letters 1112 issued by the IRS. Letter 1112 explains that the examination identified apparent weaknesses or deficiencies related to, or violations of, the BSA. Four examinations in our sample received Letter 1112 upon closure of examination outlining violations involving the areas of policies, procedures, controls, or program requirements. In addition, two exchanges had reporting and recordkeeping violations and failure to file Suspicious Activity Reports. One other case



The Internal Revenue Service Can Improve Taxpayer Compliance for Virtual Currency Transactions

exhibited conflicting information on the type of closure. The case file contained a Letter 4029 but also listed violations and referred to the issuance of Letter 1112.

Title 31 examiners did not make a significant number of FinCEN referrals

The BSA generally requires financial institutions to maintain records and to file reports that are useful in criminal, tax, or regulatory investigations, such as money laundering cases. Failure to develop and implement an anti-money laundering program, file BSA reports, or maintain records may result in criminal and/or civil penalties, depending on the nature of the violation. Criminal investigations are the responsibility of IRS Criminal Investigation, and FinCEN has the ability to assess civil penalties. BSA examiners are required to discuss any apparent violations with their manager to determine if the violations should be referred to FinCEN for consideration of penalties or other action. However, only one case from our sample had a FinCEN referral. The referred exchange failed to take corrective actions and did not sign an agreement to follow IRS recommendations and to correct anti-money laundering program, reporting, and recordkeeping violations.

The decision to refer a case to FinCEN depends upon the facts and circumstances of each case. The general standard for a FinCEN referral is significant BSA violation(s) or anti-money laundering program deficiencies. This, along with indications of willful blindness or recklessness, may warrant a referral to FinCEN. However, isolated first incidences of noncompliance normally should not be referred to FinCEN.

Generally, FinCEN disposes of many of its civil penalty cases with one of three courses of action:

- Close the case without contacting the subject of the referral.
- Issue a letter of warning or caution to the subject institution or individual.
- Assess a civil monetary penalty.

After receiving a referral, FinCEN's role includes evaluating the circumstances of the alleged violation(s) and determining whether some type of civil action, including seeking the imposition of a civil monetary penalty, should be taken against the person or financial institution.

TIGTA's September 2018 report on the BSA Program also recommended that the IRS coordinate with FinCEN on the authority to assert Title 31 penalties or reprioritize resources to more productive work. TIGTA's report found that the IRS spends considerable resources on the BSA Program; however, its impact on compliance is minimal. The IRS did not agree with the recommendation, stating that FinCEN intends to retain authority to impose Title 31 penalties to ensure consistent application across agencies. In January 2020, TIGTA officials met with FinCEN officials to discuss our finding in the September 2018 audit that the BSA Program has minimal impact on compliance and that its examiners are reluctant to refer cases for potential penalty issuance due to the perception of FinCEN inaction. As previously noted, the Acting Inspector General of the Treasury testified in 2004 that FinCEN was inconsistent and untimely in its enforcement actions and the IRS may be reluctant to refer future casino BSA violations, which was a finding on Title 31 penalty cases in our September 2018 report. We asked FinCEN officials to reconsider their decision not to allow the IRS to have penalty issuance authority; however, FinCEN officials declined to change the policy.

During this review, the Commissioner, SB/SE Division, confirmed that it would be beneficial for the IRS to have Title 31 penalty enforcement authority for BSA compliance purposes. In addition, the Commissioner stated that the IRS could increase Title 31 compliance if it had



The Internal Revenue Service Can Improve Taxpayer Compliance for Virtual Currency Transactions

penalty authority and that he was scheduling time with FINCEN officials to discuss. However, he stated that, as with any new policy, it would take resources to set up a system to assess Title 31 penalties, evaluate options, develop a process, and implement.

Title 31 examination case files did not contain all required administrative elements

Our review of seven closed Title 31 examinations found three examinations that did not have documentation that the recommended group manager concurrence meeting was held within 30 calendar days after the initial appointment meeting. Examiners at the GS-12 level and below are required to use the concurrence meeting, while GS-13 examiners are encouraged to use the meeting to provide updates on examinations and obtain guidance from managers. These three examinations involved two GS-13 and one GS-12 examiners.

These meetings are an important step in case examination because it encourages discussion between the group manager and examiner about the case, such as discussing the initial appointment meeting, developing the plan for completing the case, and any other concerns. Not conducting a timely concurrence meeting may affect the efficiency and effectiveness of an examination because the manager and examiner may miss an opportunity for airing concerns or discussing plans and strategy.

Our review found that, in two of the seven examinations we reviewed, the examiner noted the issuance and receipt of Letter 1052, *Notification of Possible IRS Check to Verify Maintenance of Required Records and Filing Reports*, in the case file notes, but the file did not include a copy of the letter.⁴⁴ Letter 1052 is a notification letter used by SB/SE Division BSA examiners to notify Non-Bank Financial Institutions that they have BSA requirements. According to the IRM, a copy of Letter 1052 should be issued to newly identified entities and a copy retained in the administrative file.⁴⁵ Additionally, the BSA examiner must verify and document in the administrative file that the financial institution received the Letter 1052 when conducting a BSA examination.

We also identified one case file that did not contain all the indicated documentation in the case file. The case file notes and lead sheets referred to an existence of other third-party reports and referred to third-party workpapers, but the case file did not include those files. The IRM requires examiners to create a well-organized and professional case file.⁴⁶ A lack of organization and/or missing information in a case file may create confusion and difficulty for review of a case by others who have no direct knowledge of the case. Additionally, failure to include attachments in the case file may cause lack of assurance that the information is indeed present in the file.

Title 31 examiners did not generally identify income tax issues and refer examinations to Title 26 examination groups

Although BSA Program examiners generally pursue Title 31 issues, they are encouraged to make referrals to the BSA Examination Case Selection for Title 26 income tax examinations if they identify issues that indicate noncompliance. The IRM prohibits BSA Program examiners from requesting records during a BSA examination for any purpose other than for conducting the BSA examination. However, if information is discovered that may be considered for a possible income tax examination, the examiner should prepare Form 5346, *Examination Information*

⁴⁴ The current title of Letter 1052 is *Bank Secrecy Act Requirements Notification Letter* (June 2013).

⁴⁵ IRM 4.26.6.2.1(1) (Nov. 14, 2006), now replaced by IRM 4.26.6.3.1(1) (Oct. 8, 2019).

⁴⁶ IRM 4.26.6.4.9(1) (Nov. 14, 2006), now replaced by IRM 4.26.6.5.4 (Oct. 8, 2019).



The Internal Revenue Service Can Improve Taxpayer Compliance for Virtual Currency Transactions

Report, to refer the issue for examination.⁴⁷ Some examples of transactions that may warrant submitting a Form 5346 are:

- Large cash deposits with inadequate records.
- The lack of cash deposits by a financial institution that usually generates large amounts of cash.
- Any other suspicious transaction that indicates the correct amount of income may not have been reported for Title 26 purposes.
- Potential structuring cases.

None of the examinations in our review had issues referred using a Form 5346. In a September 2018 report on the use of Currency Transaction Report information in examinations, TIGTA found that the IRS was not effectively tracking referrals from BSA Program examiners to the Examination function.⁴⁸ We recommended that the IRS establish formalized procedures for processing BSA Program referrals and begin formally tracking the time required to send referrals to the Field Examination Support team. The IRS agreed with the recommendation and, according to the IRS, implemented corrective action in November 2019. We found that the current training material provided to BSA Program examiners and frontline managers provides guidance to help assess whether an entity or its customers are potentially avoiding taxes and how to develop a referral without expanding the scope of the BSA examination into an income examination. The purpose of the BSA examination is not to identify information outside the scope of the BSA examination, but it is equally as important not to ignore transactions or activities that should be referred.

Recommendation 2: The Commissioner, Small Business/Self-Employed Division, should develop a process to use and monitor Title 31 virtual currency information in Title 26 examination workload.

Management's Response: The IRS agreed with this recommendation and stated that Interim Guidance Memo SBSE 04-0819-0021 provides guidance and references a monitored process for a Title 26 examiner to use FinCEN Query, which is Title 31 information. Additionally, the IRS stated that in July 2020 all FinCEN (Title 31) data were made available on its Compliance Data Warehouse, which is accessible to the Title 26 program.

⁴⁷ IRM 4.26.6.5 (2) and (3) (Nov. 14, 2006), now replaced by IRM 4.26.6.5.3.16(2) and (3) (Oct. 8, 2019).

⁴⁸ TIGTA Ref. No. 2018-30-076, *The Internal Revenue Service Still Does Not Make Effective Use of Currency Transaction Reports* (Sept. 2018).



The Internal Revenue Service Can Improve Taxpayer Compliance for Virtual Currency Transactions

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to evaluate the IRS's efforts to ensure the accurate reporting of virtual currency transactions as required under U.S.C. Titles 26 and 31. To accomplish our objective, we:

- Determined the IRS policies and procedures in place to ensure tax compliance pertaining to virtual currency.
- Determined the effectiveness of the IRS's Title 26 virtual currency exchange audits (if any) and any efforts to ensure information reporting requirements by virtual currency exchanges.
- Determined the effectiveness and compliance impact of the IRS's Title 31 virtual currency exchange examinations process.
- Assessed information reporting compliance of virtual currency exchanges by analyzing volumes of Forms 1099-K issued by the exchanges.
- Evaluated the risk for fraud, waste, and abuse to obtain reasonable assurance that improprieties do not exist in the use of virtual currency exchange data within the LB&I and SB/SE Divisions.

Performance of This Review

This review was performed with information obtained from the IRS SB/SE Division headquarters located in Lanham, Maryland, and the LB&I Division headquarters located in Washington, D.C., during the period August 2018 through June 2020. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Major contributors to the report were Mathew Weir, Assistant Inspector General for Audit (Compliance and Enforcement Operations); Linna Hung, Director; Curtis Kirschner, Acting Director; Glen Rhoades, Director; Robert Jenness, Audit Manager; and Sean Morgan, Senior Auditor.

Validity and Reliability of Data From Computer-Based Systems

We performed tests to assess the reliability of data from the IRS's Information Returns Master File and Audit Information Management System. We evaluated the data by (1) performing electronic testing of required data elements, (2) reviewing existing information about the data and the system that produced them, and (3) interviewing agency officials knowledgeable about the data. We determined that the data were sufficiently reliable for purposes of this report.



The Internal Revenue Service Can Improve Taxpayer Compliance for Virtual Currency Transactions

Internal Controls Methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: the IRS's processes for planning and carrying out examinations on virtual currency exchanges. We tested these controls by performing analyses of individual tax return data from the Information Returns Master File located on the TIGTA Data Center Warehouse and examination status on the IRS's Audit Information Management System and reviewing and analyzing virtual currency examination case files.



The Internal Revenue Service Can Improve Taxpayer Compliance for Virtual Currency Transactions

Appendix II

Management's Response to the Draft Report

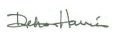


COMMISSIONER
SMALL BUSINESS/Self-EMPLOYED DIVISION

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

September 4, 2020

MEMORANDUM FOR MICHAEL E. McKENNEY
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Eric C. Hylton  Digitally signed by Geerl D. Harris
Date: 2020.09.04 15:10:59 -04'00'
Commissioner, Small Business/Self-Employed Division

SUBJECT: Draft Audit Report – The Internal Revenue Service Can Improve Taxpayer Compliance for Virtual Currency Transactions (Audit #201830034)

Thank you for the opportunity to review and comment on the subject draft report. As reflected in your report, the Internal Revenue Service (IRS) has undertaken several measures to address virtual currency tax compliance risks. We continue to engage a broad spectrum of external stakeholders for feedback on how the IRS might balance taxpayer service with the proper regulatory enforcement of digital assets, including virtual currency.

The Department of the Treasury and IRS continue efforts to close the virtual currency information gap by working to develop guidance clarifying the proper information reporting required for these types of transactions. The Department of the Treasury 2019-2020 Priority Guidance Plan includes "Guidance regarding information reporting on virtual currency under §6045," which will address third-party reporting requirements under §6045 for brokers who effect sales of virtual currency. We intend to propose rules that avoid duplicate reporting under other information reporting regimes to the extent such brokers are also Third-Party Settlement Organizations (TPSOs).

As your report recognized, in 2018 the IRS' Large Business and International Division (LB&I) announced a virtual currency compliance campaign aimed at addressing virtual currency non-compliance through a range of actions including outreach, examination, and criminal prosecution. We issued more than 10,000 letters to taxpayers with virtual currency transactions to help them understand their tax and filing obligations and have initiated numerous examinations related to virtual currency non-compliance.

In Fiscal Year (FY) 2020, we identified and selected more than 4,000 cases between our Automated Underreporter Program and nonfilers sent to our Special Enforcement Program. We plan to identify additional virtual currency cases in FY 2021. The SB/SE Division's Bank Secrecy Act (BSA) program conducts an increasing number of Virtual



The Internal Revenue Service Can Improve Taxpayer Compliance for Virtual Currency Transactions

2

Currency Exchange examinations each year. Although, the number of closures is relatively low, the closures do not account for the BSA program resources currently being expended to increase current and future coverage. The report suggests that an increase in Title 31 examinations of virtual currency exchanges could close the information reporting gap. However, BSA examiners are prohibited from accessing Title 26 information, which includes information return filings. Therefore, BSA examiners are prohibited from reviewing Title 26 information to identify virtual currency exchanges that are not complying with their Title 26 information reporting requirements.

Both in the subject report and in a report published in 2018¹, TIGTA has recommended that the IRS coordinate with FinCEN on the authority to assert Title 31 penalties. The report acknowledges, however, that FinCEN officials have declined previous attempts to change the policy on penalty issuance authority. Although we believe the IRS could increase Title 31 compliance with penalty issuance authority, significant resources would be necessary to build a penalty assessment framework. Additionally, FinCEN has numerous functional regulators who administer Title 31 enforcement activities, none of which have penalty authority. However, we have begun a dialogue with FinCEN to explore the possibility of obtaining penalty issuance authority and anticipate significant deliberation during the coming year.

Although this audit focused on work in our Examination organization, our work with virtual currency extends further. We are also adding an emerging mitigating threats team within the Office of Fraud Enforcement that will support our efforts on Cyber Currency tax fraud activities. The team will collaborate with other federal and state agencies and industry partners on emerging threats through informal discussions and interagency working groups. These interagency efforts can result in leveraging resources to maximize the outcomes to combat fraud. And for individuals and businesses with balances due, SB/SE Collection revised all Collection Information Statements (Forms 433) to include solicitation and documentation of information regarding virtual currency ownership.

In closing, we appreciate your continued input as we strive to support and improve taxpayer compliance for virtual currency transactions. Attached is a detailed response outlining our planned corrective actions. If you have any questions, please contact me or Scott Irick, Director of Examination, SB/SE Operating Division.

Attachment

¹ TIGTA, Ref. No. 2018-30-071, *The Internal Revenue Service's Bank Secrecy Act Program Has Minimal Impact on Compliance* (Sept. 2018).



The Internal Revenue Service Can Improve Taxpayer Compliance for Virtual Currency Transactions

Attachment

RECOMMENDATION 1:

The Deputy Commissioner for Services and Enforcement should continue efforts to close the virtual currency information gap by issuing guidance clarifying the proper information reporting associated with virtual currency transactions.

CORRECTIVE ACTION:

The Treasury Department and the IRS are currently working to develop guidance on third-party reporting under §6045 of the Internal Revenue Code for certain taxable transactions involving virtual currency. The current Treasury and IRS Priority Guidance Plan identifies this guidance as a shared priority. Nonetheless, we are unable to guarantee an issuance date because the process by which guidance is developed is not within our sole control.

IMPLEMENTATION DATE:

N/A

RESPONSIBLE OFFICIAL:

N/A

CORRECTIVE ACTION MONITORING PLAN:

N/A

RECOMMENDATION 2:

The Commissioner, Small Business/Self-Employed Division, should develop a process to use and monitor Title 31 virtual currency information in Title 26 examination workload.

CORRECTIVE ACTION:

Interim Guidance Memo SBSE 04-0819-0021 provides guidance and references a monitored process for a Title 26 examiner to use FinCEN Query, which is Title 31 information. Additionally, in July 2020 all FinCEN (Title 31) data is now available on the IRS's Compliance Data Warehouse (CDW) which is accessible, following protocols and internal controls, to the Title 26 program.

IMPLEMENTATION DATE:

Implemented

RESPONSIBLE OFFICIAL:

N/A

CORRECTIVE ACTION MONITORING PLAN:

N/A



The Internal Revenue Service Can Improve Taxpayer Compliance for Virtual Currency Transactions

Appendix III

Abbreviations

BSA	Bank Secrecy Act
FinCEN	Financial Crimes Enforcement Network
FY	Fiscal Year
GAO	Government Accountability Office
GS	General Schedule
I.R.C.	Internal Revenue Code
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
LB&I	Large Business and International
MSB	Money Service Business
SB/SE	Small Business/Self-Employed
TIGTA	Treasury Inspector General for Tax Administration
TPSO	Third-Party Settlement Organization
TY	Tax Year
U.S.C.	United States Code